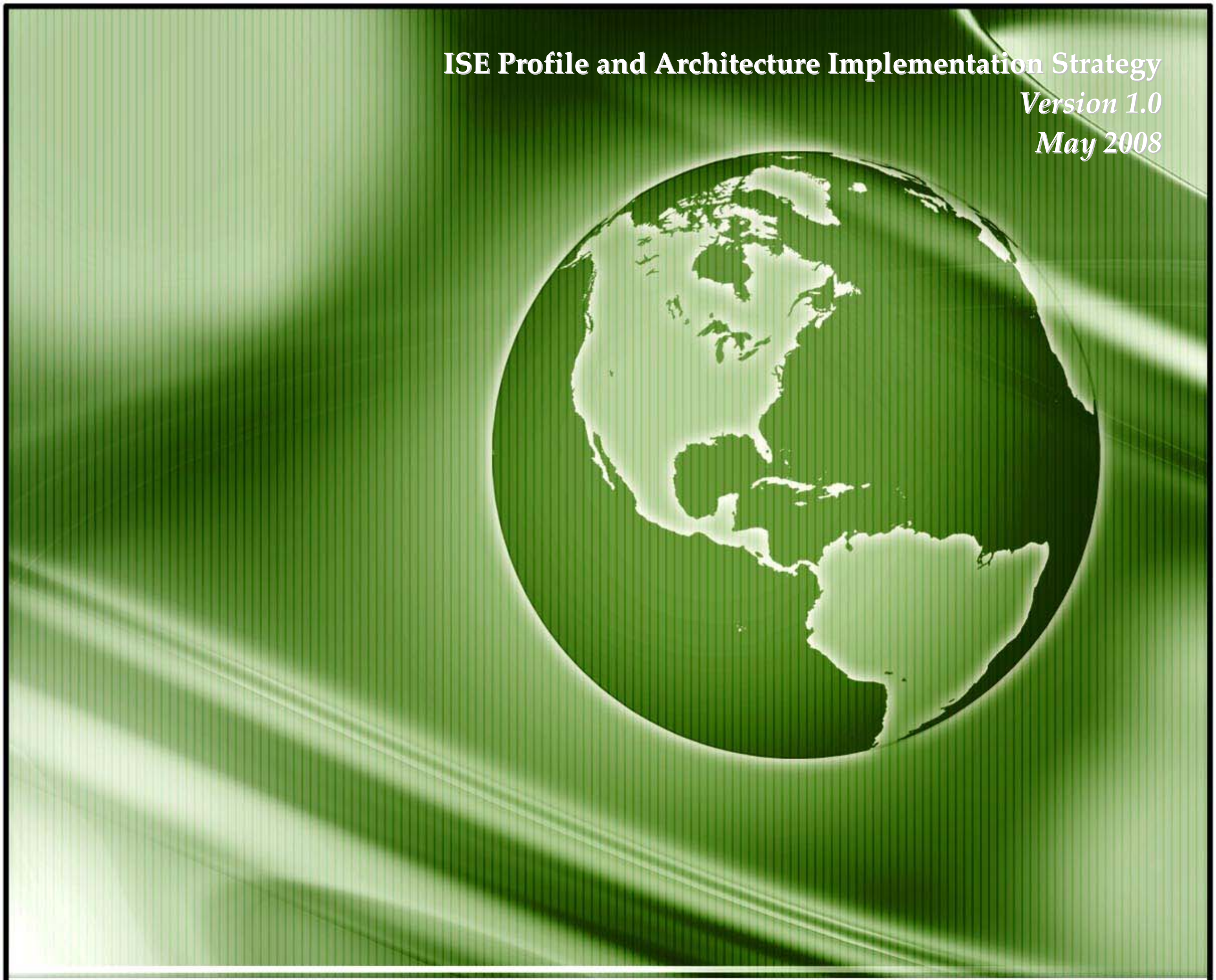


ISE Profile and Architecture Implementation Strategy
Version 1.0
May 2008

INFORMATION SHARING ENVIRONMENT PROFILE AND ARCHITECTURE IMPLEMENTATION STRATEGY

Prepared by the
Program Manager, Information Sharing Environment

This document was reviewed and approved by the Federal Architecture and Infrastructure Committee and the Office of Management and Budget to be a valid Profile and Architecture Implementation Strategy for the Information Sharing Environment.[1]

April 4, 2008

[1] See Appendix A for Architecture and Infrastructure Committee (AIC) letter.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Executive Summary

Section 1016 of the *Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004*[2] requires the President to establish an Information Sharing Environment (ISE), "for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties." Executive Order (EO) 13388, issued on October 25, 2005[3], requires that "to the maximum extent consistent with applicable law, agencies shall, in the design and use of information system(s) and in the dissemination of information among agencies (a) give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America; (ii) the interchange of terrorism information among agencies, (iii) the interchange of terrorism information between agencies and appropriate authorities of State, local, and tribal (SLT) governments and between agencies and appropriate private sector entities; and (iv) the protection of the ability of agencies to acquire additional such information; and (b) protect the freedom, information privacy, and other legal rights of Americans."

On December 16, 2005, the President issued a Memorandum for the Heads of Executive Departments and Agencies on the Guidelines and Requirements in Support of the Information Sharing Environment that included requirements to *develop a common framework for the sharing of information* between and among Executive departments and agencies and State, local and tribal governments, law enforcement agencies, and the private sector and *define common standards* for the way information is acquired, accessed, shared, and used within the ISE.[4]

To comply with legislative and Presidential direction, this ISE architectural approach builds upon processes affecting existing systems throughout the ISE, addresses terrorism-related information sharing across multiple levels of security and protection levels, and incorporates mechanisms for protecting privacy and civil liberties. The Program Manager, Information Sharing Environment (PM-ISE), introduced the ISE architecture and standards program, a cross-community, institutional approach for helping ISE participants adjust, plan, install, and operate current and future information resources that form the infrastructure fabric of the ISE. A business process-driven ISE

[2] Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law No. 108-458 (December 17, 2004). Section 1016 of IRTPA was amended on August 3, 2007 by the *Implementing Recommendations of the 9/11 Commission Act of 2007*, Public Law No. 110-53. This version of the ISE Profile and Architecture Implementation Strategy (ISE PAIS) does not address the additional authorities and requirements set forth in P.L. 110-53; these will be addressed in future versions of the ISE EAF and the ISE PAIS. The new law expands the scope of the ISE to include homeland security information and weapons of mass destruction information and sets forth additional ISE attributes. It also codifies many of the recommendations developed in response to the President's information sharing guidelines, such as the creation of the Interagency Threat Assessment and Coordination Group and the development of a national network of State and major urban area fusion centers.

[3] Executive Order 13388—Further Strengthening the Sharing of Terrorism Information to Protect Americans, found at Internet site http://www.ise.gov/docs/eo%2013388%20-%2010252005.pdf.

[4] Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment (Washington: White House, 2005), Section 1, found at Internet site http://www.whitehouse.gov/news/releases/2005/12/20051216-10.html.

Enterprise Architecture Framework (EAF) and this companion document, the ISE Profile and Architecture Implementation Strategy (PAIS), are used to implement the ISE across Federal information resources, consistent with Office of Management and Budget (OMB) FEA Framework guidelines. Furthermore, this approach defines processes for connecting information resources of SLT governments, the private sector, and foreign partners and integrates the diverse landscape of existing policies and management processes across the Federal Government. A fully functional ISE requires the development of information sharing relationships and the transformation of culture and institutions supported by the construction, integration, and sustained operations of terrorism-related information sharing systems, processes, networks, services, and other resources across the Nation.

Document Organization

This ISE PAIS is a companion document to the ISE EAF and provides implementation guidance for ISE participants. As Table ES-1 outlines, this ISE PAIS is one of three documents necessary to define the architecture program of the ISE.

Table ES-1. ISE Architecture Program Documentation

Title	Description
ISE EAF	A high-level description of the components, structure, and unifying characteristics of the ISE to include the four partitions: Business, Data, Application & Service, and Technical.
ISE PAIS	A guide for ISE participants that describes what each must do to connect to the ISE, expose data to the ISE, and access data and services provided by the ISE.
ISE Drivers and Requirements Specification	A high-level specification of the ISE requirements. Requirements are allocated to components of the ISE EAF including an ISE participant's Shared Space, ISE Core Transport, ISE Core Services, and ISE Portal.

Chapter 1: Introduction

The introduction describes high level background information. It defines the purpose and scope of this document. It also provides descriptions of planning, issuances, governance, and trust considerations and the way these factors all affect ISE architecture efforts. Finally, this chapter provides the methods used to test and evaluate ISE-consistent architectures.

Chapter 2: ISE Program Management Approaches

This chapter provides brief descriptions of the fundamental tools and approaches required to develop and implement the ISE. These tools and approaches include risk management, information security, information flow implementation, and integration with enterprise architectures. Additionally this chapter outlines approaches to service-based architecture, data standardization, and architecture patterns.

Chapter 3: ISE Architecture Implementation Life Cycle

This chapter provides a detailed description of the iterative architectural process used to develop and implement the ISE architecture. It outlines, in detail, the activities and anticipated inputs and outputs/outcomes at each stage of the ISE architecture development process.

Appendix A: Architecture and Infrastructure Committee Letter

This appendix provides the actual letter from the AIC approving this document to be a valid Profile and Architecture Implementation Strategy for the ISE.

Appendix B: Acronyms

This appendix provides an explanation of the acronyms used in this document.

Appendix C: Bibliography

This appendix provides a list of the major sources referenced in this document.

Appendix D: Glossary

This appendix provides definitions for certain specialized terms used in this document.

Appendix E: ISE Business Processes

This appendix provides definitions for the specialized terms used in this document with respect to defining ISE-related business processes.

Appendix F: Summary of Recommended Actions

This appendix provides a summarized list of recommended actions for Implementation Agents and other ISE participants cited in this document.

This page intentionally blank.

Chapter 1 – Introduction

1.1 Purpose and Scope

This ISE PAIS helps drive ISE participants' enterprise architectures (EAs), segment architectures, solution architectures, and systems that follow key activities of the OMB Capital Planning and Investment Control (CPIC) processes, as illustrated below in Figure 1-1. Each ISE participant can use the guidance herein and the Federal Transition Framework (FTF) Catalog to develop processes, approaches, and artifacts for an ISE participant to implement and build an operational, compliant ISE segment architecture, including an ISE Shared Space. Similarly, both Federal and non-Federal ISE participants can use this guidance to develop their related information resource capital planning and investment processes for interfacing into the ISE and also to align their standards, processes, and policies to those of other Federal partners.

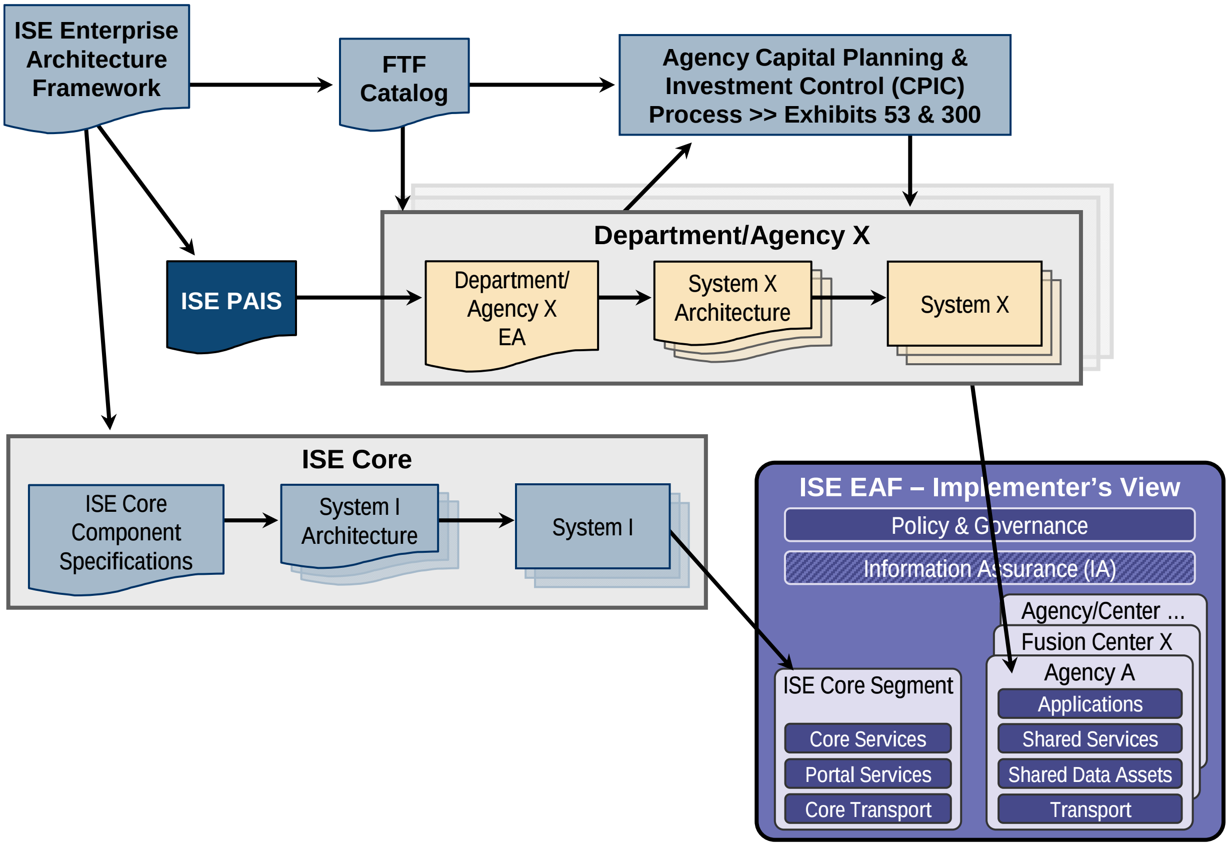


Figure 1-1. Using the ISE PAIS

This ISE PAIS recognizes and leverages the ISE EAF as an approved and accepted framework for structuring and describing information sharing services, systems, and processes required for an organization to participate in the ISE. Recognizing that establishing trust (to include proper application of information assurance [IA]) is critical in the implementation of a protected and trusted ISE, this ISE PAIS includes guidance for incorporating a common risk management framework, trustworthiness, governance, and information system(s) security concepts (including considerations for security and protecting privacy and civil liberties) into ISE participants' and Implementation Agents' EAs.

Moreover, this ISE PAIS provides guidance to ISE participants and Implementation Agents for developing and implementing a successful and operational ISE. An ISE participant refers to Federal agencies, State and major urban area fusion centers, and private sector and foreign partners that take part in the ISE. An ISE Implementation Agent refers to an organization responsible for providing additional infrastructure and services in the Core Segment as defined in the ISE EAF.

1.2 Planning Issuances, Governance, and Trust

The existing ISE governance structure is depicted in Figure 1-2 below. Further explanation of ISE governance is outlined in Chapter 4 of the ISE Implementation Plan.

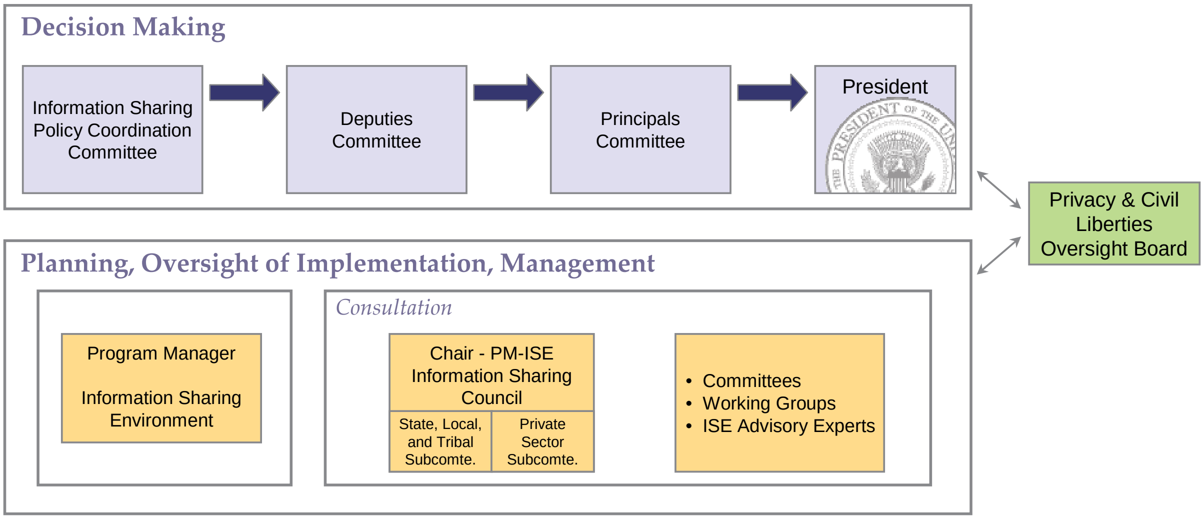

Decision Making
Information Sharing Policy Coordination Committee
Deputies Committee
Principals Committee
President
Privacy & Civil Liberties Oversight Board
Planning, Oversight of Implementation, Management
Program Manager
Information Sharing Environment
Consultation
Chair - PM-ISE Information Sharing Council
State, Local, and Tribal Subcomte.
Private Sector Subcomte.
• Committees
• Working Groups
• ISE Advisory Experts

Figure 1-2. ISE Governance

Achieving the target state of the ISE will likely require changes in policies, a governance process suitable for a broad range of organizations and jurisdictions, and processes for establishing and maintaining trust among participants. A description of trustworthiness of information systems supporting the ISE is also provided in section 2.1.3 of this ISE PAIS, highlighting relationships among policies, governance, risk management, and trust. Participation by ISE participants in relevant working groups and committees is encouraged.

1.3 Leveraging Efforts

To capitalize on the critical inter-organizational processes associated with ISE architecture and standards efforts, the PM-ISE and Federal departments and agencies developed the following key documents that are being leveraged to produce this ISE PAIS. The ISE PAIS cuts across the interrelated FEA reference models providing guidance to Federal departments and agencies for use in implementing the ISE. The ISE PAIS is not only based on the ISE EAF but also includes guidance and requirements from the ISE Implementation Plan.

1.3.1 ISE Implementation Plan

On November 16, 2006, and pursuant to the President's delegation of such authority, the Director of National Intelligence (DNI) submitted to Congress the *ISE Implementation Plan (IP)*[5]*.* The IP provided an initial description of the ISE plans, policies, requirements, and governance structure. The Implementation Plan introduced ISE architecture and standards to help ISE participants plan, install, and operate their information resources in a manner that will contribute components of their internal infrastructures into the physical instantiation of a nationwide counterterrorism ISE.[6] While participants in the ISE continue to be responsible for their own counterterrorism missions and systems supporting these missions, the physical ISE will support improvements to individual counterterrorism business processes and capabilities through increased access to terrorism information across the ISE community.

1.3.2 ISE Enterprise Architecture Framework

The PM-ISE has developed the ISE Enterprise Architecture Framework (ISE EAF), and published Version 1.0 on August 30, 2007, in a manner that builds upon existing Federal Government policies, standards, procedures, programs, systems, and architectures and with the objective of establishing a decentralized, comprehensive, and coordinated environment[7]. The ISE EAF and supporting Common Terrorism Information Sharing Standards (CTISS) will help improve information sharing practices, reduce barriers to sharing, and institutionalize information sharing. Cross-ISE in nature, the ISE EAF will provide descriptions of ISE business processes, information flows and relationships, services, and exchange relationships. Overall, the ISE EAF meets three objectives: (1) provides a comprehensive, strategic description of the overall ISE architecture; (2) establishes an architectural framework for implementing ISE capabilities; and (3) identifies key architectural decisions that have been made or must be made. The ISE EAF will drive long-term ISE technology improvement and

[5] Office of the PM-ISE, Information Sharing Environment Implementation Plan, November 2006, found at Internet site http://www.ise.gov.

[6] 44 U.S.C. 3502(6) defines information resources as "information and related resources, such as personnel, equipment, funds, and information technology."

[7] The Office of Management and Budget (OMB) has suggested the term "enterprise architecture framework" for the ISE rather than "enterprise architecture" because the ISE EAF is a cross-agency construct providing guidance to agencies developing the information sharing components of their enterprise architectures.

information system(s) planning, investing, and integration to support the effective conduct of U.S. counterterrorism activities. The applicable types of information that traverse the ISE include terrorism information,[8] homeland security information,[9] and law enforcement information.[10]

Table 1-1 depicts the hierarchical relationships among the various levels of architectures used within individual agencies and organizations across the ISE that are influenced by the ISE EAF and this ISE PAIS. Consistent with OMB guidance, frameworks and profiles, enterprise, segment,[11] and solution architectures[12] provide different perspectives and levels of detail for agencies and organizations in their enterprise architecture planning. At the highest level, frameworks provide logical structures for classifying and organizing complex enterprise architecture information, and, specifically, the Federal Enterprise Architecture Framework (FEAF) provides "a structure for organizing Federal resources and for describing and managing Federal Enterprise Architecture activities."[13] The ISE EAF, in turn, presents a logical structure of ISE business processes, information flows and relationships, services, and high-level data partition descriptions and exchange relationships.

[8] The term "terrorism information" means "all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to(i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (iii) communications of or by such groups or individuals; or (iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals." [IRTPA, Section 1016(a)(5), as amended.]

[9] The term "homeland security information" means any information possessed by a Federal, State, or local agency that (a) relates to the threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) improves the identification or investigation of a suspected terrorist or terrorist organization; or (d) improves the response to a terrorist act. [Section 892(f)(1) of the Homeland Security Act (6 U.S.C. 482(f)(1)).]

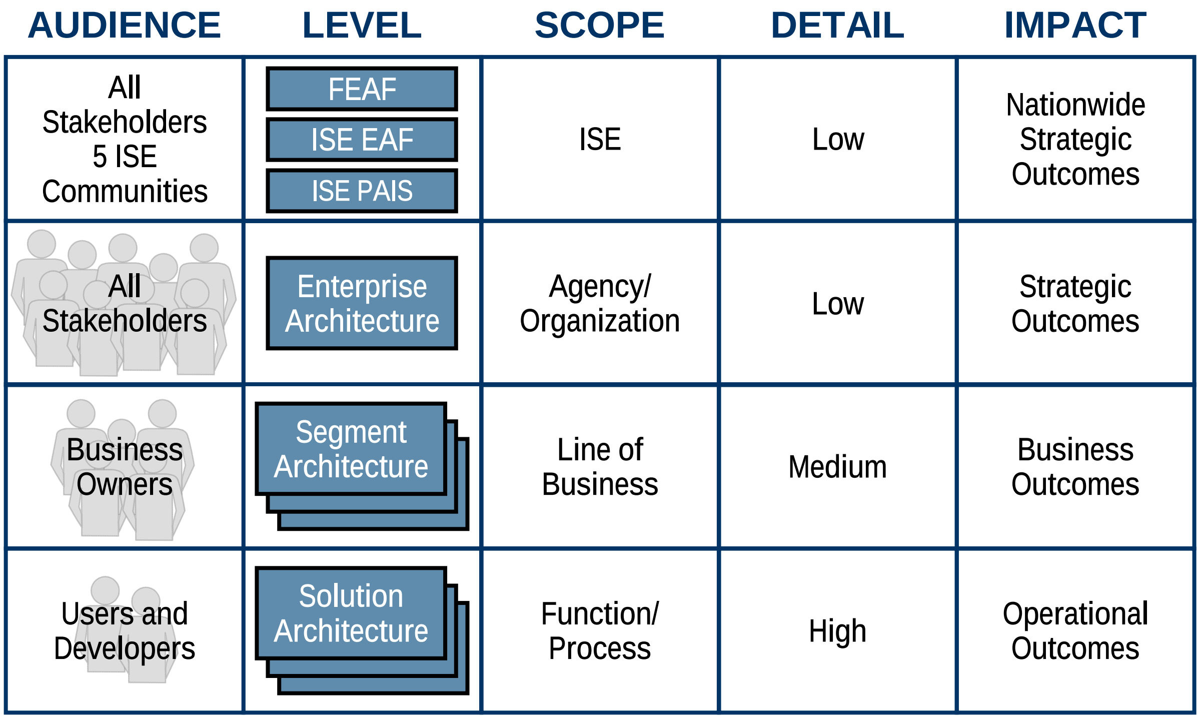
[10] For the purposes of the ISE, law enforcement information addresses any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance. [Extracted from the Recommendations for Presidential Guideline 2.]

[11] Segment architecture refers to a business driven approach to defining and designing, in addition to other supporting architectural components, each participant's ISE Shared Space. It leverages the FEA consolidated reference model, the ISE EAF, and the FTF catalog to build a layered architecture.

[12] Solution architecture refers to a business driven approach to developing shareable assets and IT components in support of business processes identified in the ISE EAF and participant segment architectures.

[13] CIO Council, Federal Enterprise Architecture Framework, Version 1.1, (CIO Council: Washington, DC, 1999), C-6, found at Internet site http://www.cio.gov/Documents/fedarch1.pdf.

Table 1-1. Levels of Architecture



AUDIENCE	LEVEL	SCOPE	DETAIL	IMPACT
All Stakeholders 5 ISE Communities	FEAF ISE EAF ISE PAIS	ISE	Low	Nationwide Strategic Outcomes
All Stakeholders	Enterprise Architecture	Agency/ Organization	Low	Strategic Outcomes
Business Owners	Segment Architecture	Line of Business	Medium	Business Outcomes
Users and Developers	Solution Architecture	Function/ Process	High	Operational Outcomes

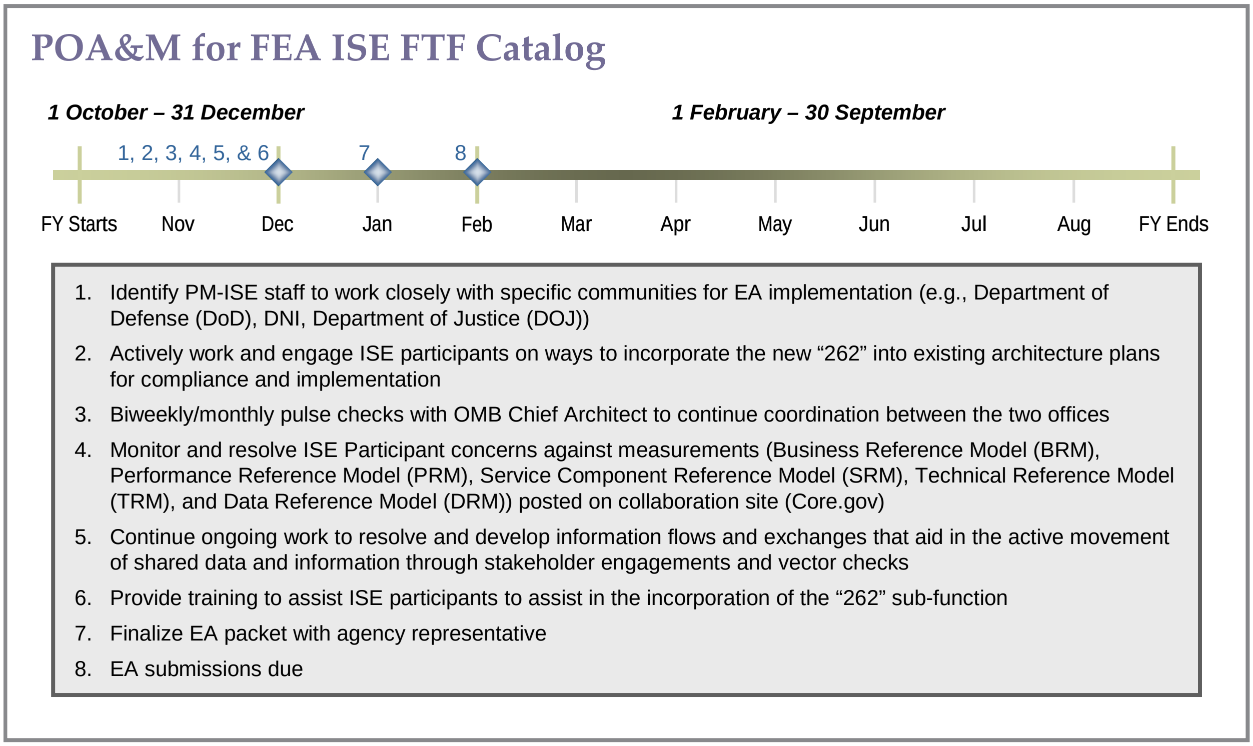
1.3.3 OMB FTF Catalog

The Federal Transition Framework (FTF) Catalog[14] is an OMB compliance tool used to oversee and align CPIC processes to interpret Government-wide IT policy objectives and cross-agency initiatives. The FTF Catalog provides a simple structure to organize and publish existing information to (1) enhance the quality and consistency of information on cross-agency initiatives, (2) increase the level and speed of adoption of cross-agency initiatives, and (3) improve the overall effectiveness and efficiency of IT investments and programs related to cross-agency initiatives. In prior years, OMB has posted the FTF Catalog on its home page. In August 2007, OMB decided to leverage an online collaborative website, Core.gov, for posting FTF Catalog information. Core.gov grew from an initiative within the Federal Enterprise Architecture (FEA) Project Management Office (PMO) to support the need to perform cross-agency collaboration, transformation, and Government-wide improvement collaboration seamlessly and easily.

[14] Details of the Federal Transition Framework can be found at Internet site http://www.whitehouse.gov/omb/egov/a-2-EAFTF.html.

The ISE section of the FTF Catalog[15] provides ISE Implementation Agents and ISE participants the ability to discover and search on mission relevant initiatives and deliveries at a wider glance. This provision increases the ISE participants' abilities to leverage existing and proven capabilities while minimizing cost, resources, and time to create and implement new capabilities.

Figure 1-3, below, represents the key activities that the PM-ISE (in conjunction with the FEA Program Management Office in OMB) will support toward accurate accountability and incorporation of the new Information Sharing sub-function and other elements of the ISE EAF and ISE PAIS. These activities also identify the stages traversed to support ISE participant enterprise architecture and segment architecture development, preparation, and submission during annual OMB EA budget reviews.



1. Identify PM-ISE staff to work closely with specific communities for EA implementation (e.g., Department of Defense (DoD), DNI, Department of Justice (DOJ))
2. Actively work and engage ISE participants on ways to incorporate the new "262" into existing architecture plans for compliance and implementation
3. Biweekly/monthly pulse checks with OMB Chief Architect to continue coordination between the two offices
4. Monitor and resolve ISE Participant concerns against measurements (Business Reference Model (BRM), Performance Reference Model (PRM), Service Component Reference Model (SRM), Technical Reference Model (TRM), and Data Reference Model (DRM)) posted on collaboration site (Core.gov)
5. Continue ongoing work to resolve and develop information flows and exchanges that aid in the active movement of shared data and information through stakeholder engagements and vector checks
6. Provide training to assist ISE participants to assist in the incorporation of the "262" sub-function
7. Finalize EA packet with agency representative
8. EA submissions due

Figure 1-3. Notional Plan of Action and Milestones (POA&M) for FEA, ISE, FTF Catalog

In consultation with Information Sharing Council (ISC) departments and agencies, the PM-ISE will coordinate OMB EA, Exhibit 53/300, and Budget Reviews according to the processes identified in the following Figure 1-4, which depicts a general department and agency timeline regarding budget/investment activities and OMB deadlines.

[15] The current FTF Catalog may be viewed at http://www.whitehouse.gov/omb/egov/a-2-EAFTF.html.

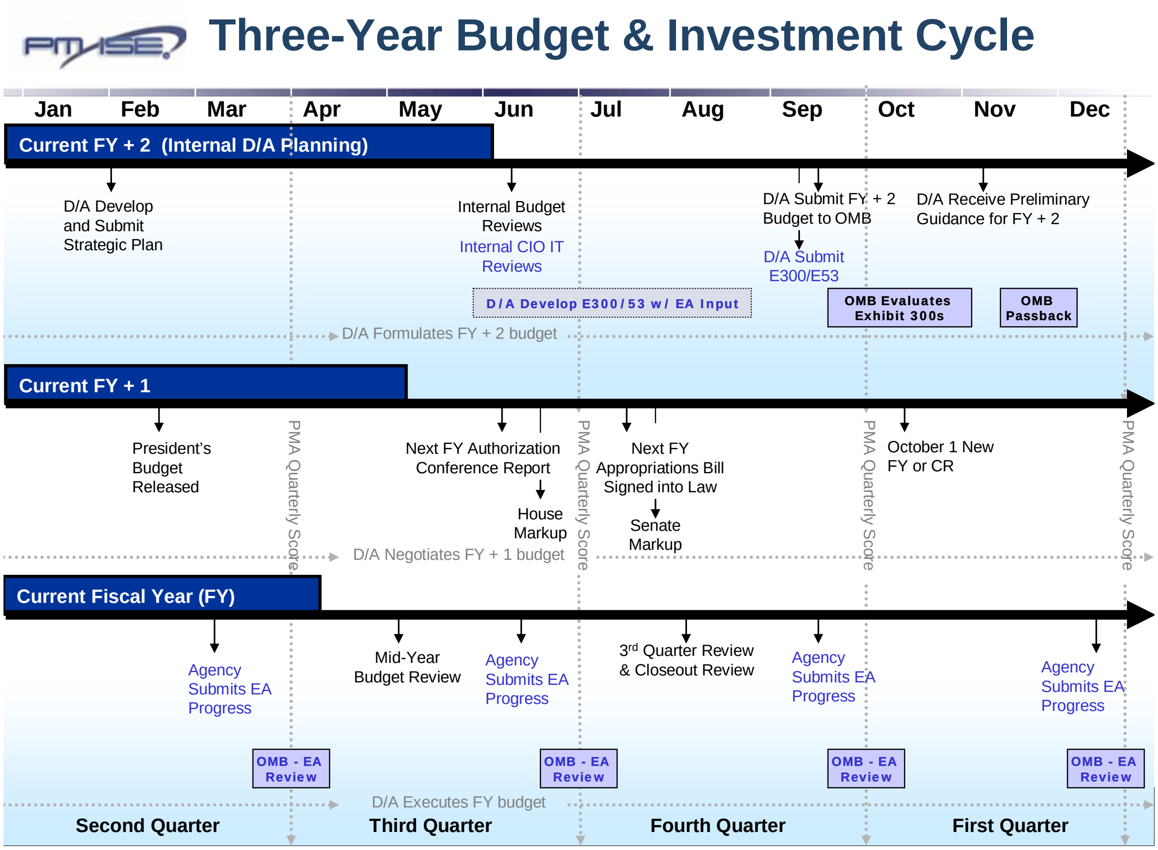

Three-Year Budget & Investment Cycle
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Current FY + 2 (Internal D/A Planning)
D/A Develop and Submit Strategic Plan
Internal Budget Reviews
Internal CIO IT Reviews
D/A Submit FY + 2 Budget to OMB
D/A Submit E300/E53
D/A Receive Preliminary Guidance for FY + 2
D/A Develop E300/53 w/ EA Input
OMB Evaluates Exhibit 300s
OMB Passback
D/A Formulates FY + 2 budget
Current FY + 1
President's Budget Released
Next FY Authorization Conference Report
House Markup
Next FY Appropriations Bill Signed into Law
Senate Markup
October 1 New FY or CR
PMA Quarterly Score
PMA Quarterly Score
PMA Quarterly Score
PMA Quarterly Score
D/A Negotiates FY + 1 budget
Current Fiscal Year (FY)
Agency Submits EA Progress
Mid-Year Budget Review
Agency Submits EA Progress
3rd Quarter Review & Closeout Review
Agency Submits EA Progress
Agency Submits EA Progress
OMB - EA Review
OMB - EA Review
OMB - EA Review
OMB - EA Review
D/A Executes FY budget
Second Quarter
Third Quarter
Fourth Quarter
First Quarter

Figure 1-4. Department and Agency Activities Toward OMB Budget Deadlines

1.4 Testing and Evaluation

For each security domain (TS/SCI, Secret/Collateral, SBU), an environment for testing, integrating, and managing ISE components must be established to ensure that proposed components of the ISE are interoperable to the extent intended and compliant with ISE standards and requirements. Compliance with security, including privacy, and section 508 requirements are also vital for a successful evaluation in addition to functional, operational, and performance requirements for enabling associated business processes. The environment(s) will support controlled testing, integration, security assessment, and authorization to operate within the ISE, configuration management, and verification of procedures. Facilities to capture and analyze implementation test data will support various levels of testing. Compliance with ISE common standards, as documented in the CTISS, will be evaluated when applicable.

As described in the *ISE Implementation Plan*,[16] the National Counterterrorism Center (NCTC) provides a potential platform for developing and evaluating solutions to Federal information sharing issues. The PM-ISE will designate one or more organizations and locations to establish those necessary Test and Evaluation (T&E) environments.

1.5 Privacy and Civil Liberties

Written in accordance with Presidential Guideline 5, the ISE Privacy Guidelines implement the requirements of Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 and of Section 1 of Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*. These guidelines provide the foundation for sharing information in the ISE in a manner that protects privacy and civil liberties. The guidelines balance the dual imperatives of sharing terrorism information and protecting privacy and civil liberties by establishing uniform procedures to implement required protection in unique legal and mission environments. In addition, this framework establishes an ISE privacy governance structure for deconfliction, compliance, and continuous development of privacy guidance.[17]

The privacy guidelines build on a set of core principles that all ISE participants will follow. These principles require specific, uniform action across these entities and reflect basic privacy and civil liberty protections and best practices, requiring ISE participants to identify any privacy-protected information to be shared; enable other ISE participants to determine the nature of the information (e.g., whether it contains information about U.S. persons); assess and document applicable legal and policy rules and restrictions that establish security, accountability, and audit mechanisms; implement data authenticity and integrity and, where appropriate, redress procedures; identify an ISE Privacy Official to ensure compliance with the guidelines; document privacy and civil liberties protections in an ISE privacy policy; and facilitate public awareness of these protections as appropriate.[18]

Successful implementation of the guidelines requires a governance structure, both to monitor compliance and to iterate guideline modifications as appropriate. The guidelines require all ISE participants to designate a senior “ISE Privacy Official” to directly oversee implementation of the guidelines. The guidelines also provide for an ISE Privacy Guidelines Committee, consisting of ISE privacy officials, to ensure consistency and standardization (where feasible) in implementation as well as to share best practices and resolve inter-agency issues.

[16] Program Manager, Information Sharing Environment, Information Sharing Environment Implementation Plan, November, 2006, Section 3.5, found at Internet site http://www.ise.gov/docs/ise-impplan-200611.pdf.

[17] Program Manager, Information Sharing Environment, Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment, found at Internet site http://www.ise.gov/docs/ise%20privacy%20guidelines%2012-4-06.pdf.

[18] Program Manager, Information Sharing Environment, Ibid.

The ISE Privacy Guidelines provide that federal agencies and the Program Manager's office will work with non-Federal entities (State, local and tribal governments, the private sector, and foreign partners and allies) to ensure that such entities develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in the guidelines[19].

[19] Program Manager, Information Sharing Environment, Ibid.

This page intentionally blank.

Chapter 2 – ISE Program Management Approaches

2.1 Information Assurance/Information Technology Security

Information security[20] is the protection of information and information system(s) from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Information security covers all aspects of an information system(s) (people, processes, and technology) and all actions necessary (protect, detect, and respond) to adequately mitigate negative impacts to the organization, individuals, other organizations, or the Nation resulting from use of the information system(s). Information security includes use of management and operational and technical safeguards and countermeasures including access control; identification and authentication; auditing and accountability; system and communications protection; incident response; contingency planning; system and information integrity; physical and environmental protection; personnel security; risk assessment; certification, accreditation, and security assessment; configuration management; awareness and training; maintenance; systems and services acquisition; planning; and media protection.

Effective information security within the ISE requires a common risk management framework, trustworthiness of information system(s), consistent policies and standards, effective governance, and appropriate training.

2.1.1 Risk Management

The ISE manages the risk associated with the sharing of information among ISE participants by employing a *Risk Management Framework (RMF)*. The RMF provides ISE participants with a disciplined, structured, flexible, extensible, and repeatable process for achieving agreed-upon degrees of trustworthiness for ISE information system(s) (see Section 2.1.3 for the definition of information system(s) trustworthiness). The RMF, which operates within the context of the architecture development life cycle, can be applied to both new and legacy information system(s) that are part of the ISE. The RMF incorporates well-defined information security standards and guidelines to facilitate the sharing of information and to demonstrate compliance with the ISE information security requirements. The plug-and-play nature of the RMF allows other entities (e.g., State, local and tribal governments, private sector) to use the framework either with National Institute of Standards and Technology (NIST) and/or Committee on National Security Systems (CNSS) security standards and guidelines or with equivalent national or international standards approved by the appropriate ISE Information Security Governance function(s) using standard criteria and categories. This RMF lends the

[20] Information security (or information system(s) security) is the term most widely used in the public and private sectors with the equivalent term within the national security community being ”Information Assurance” (IA). Within this document the term “Information Security” is used, understood to be essentially equivalent to IA as defined in Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, Revised June 2006.

extensibility to reuse and leverages other types of reporting processes already in place for ISE participants in the submission of Federal Budget submissions (i.e., the Exhibit 300). The RMF consists of the following steps:

- **Categorize** the ISE information system(s) and the information residing within the system based on the security category recommendations from the appropriate ISE Information Security governance function(s). This categorization must consider the potential impacts from not sharing the information as well as potential impacts if the information is shared. (*See Section 3.3: Identify and Categorize Candidate Assets for Sharing*).
- **Select** an agreed-to set of safeguards and countermeasures for ISE information system(s) based on the security categorization and the recommendations from the ISE Information Security Governance Board. (*See Section 3.4: Plan Transition to Information Sharing Environment*)
- **Supplement** the agreed-to set of safeguards and countermeasures based on an assessment of ISE participant's site-specific risk conditions including organization-specific security requirements, specific and credible threat information, cost-benefit analyses, or special circumstances. (*See Section 3.4: Plan Transition to Information Sharing Environment*)
- **Document** the set of safeguards and countermeasures in the ISE information system(s) security plan including the rationale for any refinements or adjustments to the implemented set of safeguards and countermeasures based on ISE participant's site-specific conditions. (*See Section 3.4: Plan Transition to Information Sharing Environment*)
- **Implement** the safeguards and countermeasures in the ISE information system(s). *(See Section 3.5: Develop and Enhance Information Technology Components.)*
- **Assess** the safeguards and countermeasures for effectiveness using appropriate methods and procedures to determine the extent to which the safeguards and countermeasures are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the ISE system. This step is key to demonstrating the degree of "trustworthiness" of the system, a critical input to the risk decision and maintenance of trust within the ISE (see Section 2.1.2 below). *(See Section 3.6: Integrate Information Technology Components into the ISE.)*
- **Authorize** the ISE information system(s) operation (with implemented safeguards and countermeasures) based upon a determination that the risk to the ISE participant's operations and assets, to individuals, to other organizations (that are part of the ISE partnership), and to the Nation resulting from the operation of the system is acceptable. *(See Section 3.6: Integrate Information Technology Components into the ISE.)*

- **Monitor** and assess agreed-to set of safeguards and countermeasures in the ISE information system(s) on a continuing basis, including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate ISE officials on a regular basis. *(See Section 3.7: Operate, Maintain, and Evaluate the ISE.)*

Figure 2-1 illustrates the specific activities in the ISE Risk Management Framework and the National Institute of Standards and Technology (NIST) security standards and guidelines associated with each activity.

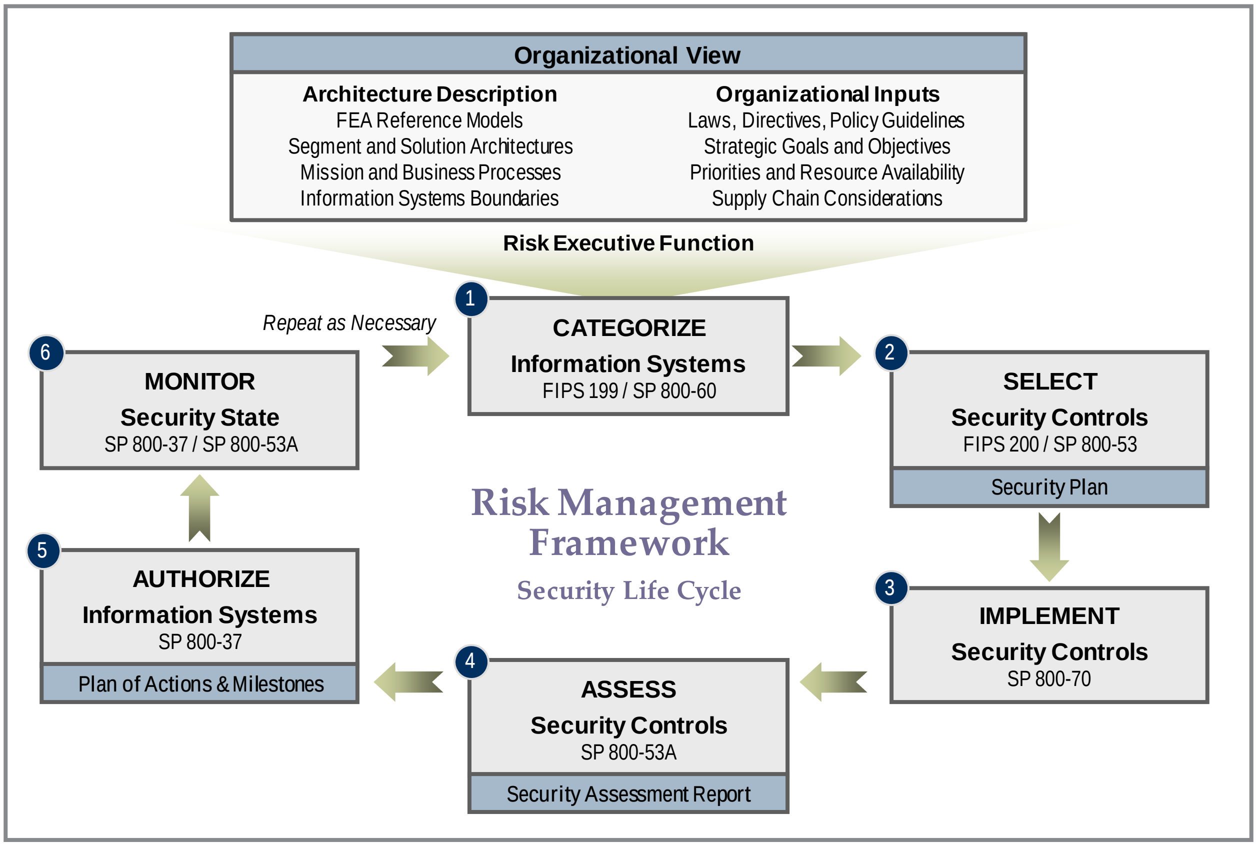


Figure 2-1. The ISE Risk Management Framework (RMF)

2.1.2 Security Categorization of ISE Information

Information will be assigned to a designated security category depending on the criticality or sensitivity of the information. The security category of the information and refined business rules and policies are major factors in determining the appropriate level of protection needed for ISE information system(s) processing, storing, or transmitting such information within the three information technology (IT) security domains (SBU, Secret, Top Secret/SCI). ISE Information Security Governance will determine the security categories of ISE information. *(See Section 3.3: Identify and Categorize Candidate Assets for Sharing.)*

2.1.3 Trustworthiness of Information System(s) Supporting the ISE

Trustworthiness is a characteristic or property of an ISE information system(s) that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system. Trustworthiness defines the security state of the ISE information system(s) at a particular point in time. Trustworthy ISE information system(s) are systems that are worthy of being trusted to operate within defined levels of risk to organizational operations and assets, individuals, other organizations, or the Nation, despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation.

Several factors can affect the trustworthiness of an ISE information system(s) including (i) the security functionality (i.e., security-related functions or features of the ISE system); (ii) the quality of the design, development, implementation, and operation of the ISE system (i.e., the degree to which the functionality is correct, always invoked, cannot be bypassed, and resistant to tampering); and (iii) the security assurance (i.e., the grounds for confidence that the claims made about the functionality and quality of the ISE system are being met).[21] Security functionality can include, for example, identification and authentication mechanisms, access control mechanisms, auditing mechanisms, and encryption mechanisms. Overall quality and efficiency of the ISE is increased by employing well-defined security policy models; structured, disciplined, and rigorous hardware and software development techniques; mechanisms for integrity such as availability, authentication, and non-repudiation; and good system/security engineering principles and concepts when building an ISE information system(s) from information technology component products. An agreed level of security assurance can be obtained from a variety of sources including, but not limited to, evidence brought forward regarding the design, development, implementation, and operation of the ISE information system(s); the results of independent assessments (e.g., analyses, testing, evaluation, inspections, and audits) of the system conducted by qualified assessors; and the results of security incident reporting and remediation activities.

Understanding trustworthiness is important to ensuring that ISE information system(s) are able to provide an appropriate degree of protection from cyber threats commensurate with the goals and objectives of the ISE and the potential adverse effects on organizations, individuals, and the Nation should there be a breach in ISE systems and a loss of confidentiality, integrity, or availability. A general expectation is that the degree of trustworthiness of an ISE information system(s) should increase as the criticality and sensitivity of the ISE information increases. ISE information system(s) processing, storing, or transmitting information that is critical or highly sensitive (to include information with a national security classification) should be highly trustworthy and expected to exhibit a high degree of penetration resistance against a wide range of

[21] Functionality, quality, and assurance requirements are described in NIST Special Publication 800-53. The ISE Information Security Governance Board will provide additional guidance on the specific requirements for safeguards and countermeasures for ISE information system(s).

adversaries with varying degrees of sophistication in cyber attacks employed against a given ISE system. Most ISE information system(s) processing, storing, or transmitting information of lesser criticality or sensitivity can be less trustworthy and provide a lesser degree of penetration resistance. The maximum acceptable level of risk to the ISE participant's operations and assets, individuals, other organizations, and the Nation and the overarching need to share information because of compelling operational requirements, guides the degree of trustworthiness needed. The trustworthiness of ISE information system(s) is an important consideration in establishing trust relationships among ISE participants, with the degree of trustworthiness directly affecting the nature of the trust relationships that are likely to be established. *(See Section 3.4: Plan Transition to Information Sharing Environment.)*

A related issue is application security. An applications security program, with specific elements to be defined, will also contribute to the development and maintenance of trust relationships among ISE participants and systems.

2.1.4 Assessing the Effectiveness of Safeguards and Countermeasures for ISE Information System(s) (Including Auditing and Authorization Requirements)

To achieve agreed-upon degrees of trustworthiness of ISE information system(s), it is necessary to determine the effectiveness of agreed-to sets of safeguards and countermeasures employed within those systems. Upon successful implementation of the appropriate safeguards and countermeasures, these controls will be able to operate as intended and produce the desired outcome with respect to meeting the security requirements for the system. Understanding the overall effectiveness of the safeguards and countermeasures implemented in the ISE information system(s) is essential in determining the risk to the ISE organization's operations and assets, individuals, other organizations, and the Nation resulting from the operation of the system and the sharing of information. Security assessments promote a better understanding of risks associated with sharing information and create more complete, reliable, and trustworthy information for ISE participants to support information sharing activities and compliance with ISE security requirements.

ISE participants are encouraged, whenever possible, to employ assessment results and related documentation available on ISE information system(s) components from independent or third party testing organizations. Today, product testing, evaluation, and validation are routinely conducted on cryptographic modules and general-purpose information technology products such as operating systems, database systems, firewalls, intrusion detection devices, Web browsers, Web applications, smart cards, biometrics devices, personal identity verification devices, network devices, and hardware platforms using national and international standards. These types of product-level assessments provide a more in-depth examination of the security features provided by the products at a level of depth and rigor that is not practical in most ISE information system(s) assessments. *(See Section 3.6: Integrate Information Technology Components into the ISE.)*

2.1.5 Trust Relationships Among ISE Participants

The timely sharing of ISE information among Federal, State, local, and tribal governments as well as foreign partners and private sector entities is a fundamental tenet of the ISE. The sharing of information depends on trust relationships and reciprocating accreditation established among the participating partners in the ISE. Trust cannot be conferred upon ISE partners; it must be earned. Trust is earned by the prospective ISE partners by (i) identifying the common goals and objectives for sharing information; (ii) agreeing upon the risk associated with the information sharing activities; (iii) agreeing upon the degree of trustworthiness needed for the ISE information system(s) processing, storing, or transmitting shared information in order to adequately mitigate the risk; (iv) determining if the respective implementations of the ISE information system(s) are worthy of being trusted to operate within the agreed-upon levels of risk despite environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation; and (v) providing ongoing monitoring and oversight to ensure that the ISE trust relationship is being maintained.

Trust relationships among ISE participants depend on carrying out each of the five elements of trust described above. The objective is to achieve an *understanding* of the prospective ISE partner's information security programs and information system(s) and to agree upon a level of security necessary to establish cross-enterprise information sharing. Levels of security depend on the consistent plans and *actions* taken by the ISE participants to provide the appropriate safeguards and countermeasures for the ISE information system(s) supporting the ISE partnerships and the *evidence* produced by the ISE partnering organizations demonstrating the effectiveness of those safeguards and countermeasures. This evidence should detail the effectiveness of safeguards and countermeasures through key documents such as the information system(s) security plan(s) (SSP), security assessment reports, and plans of actions and milestones (POA&M).[22]

Figure 2-2 illustrates the types of evidence that can be used to support the establishment of trust relationships.

[22] Information system(s) security plans, security assessment reports, and plans of action and milestones are used by authorizing officials to make authorization decisions, understanding and explicitly accepting enterprise risk. The documents are generated during the execution of the Risk Management Framework described in Section 2.1.

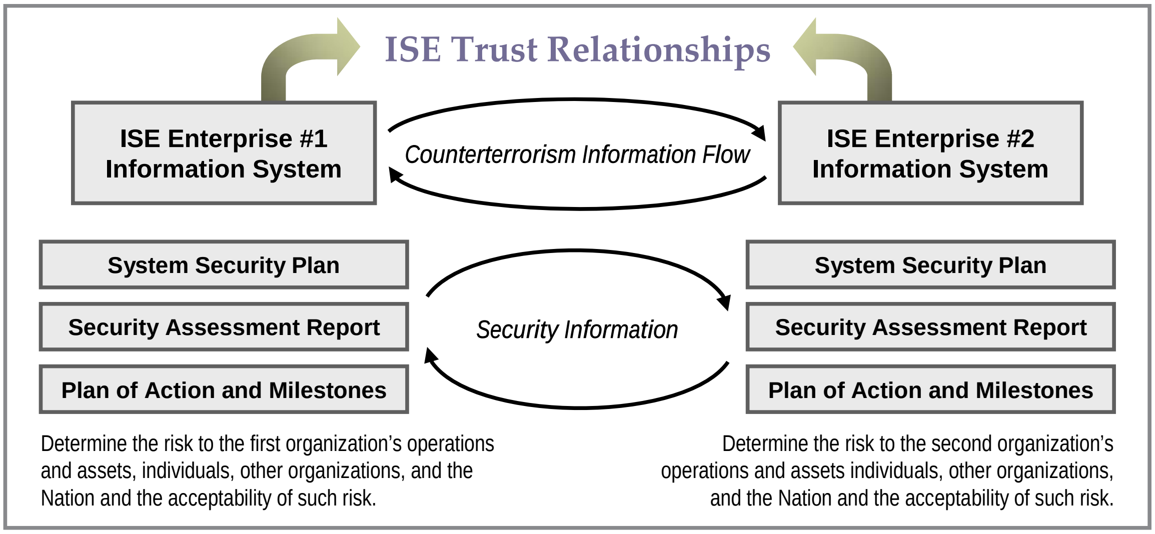

ISE Trust Relationships
ISE Enterprise #1 Information System
Counterterrorism Information Flow
ISE Enterprise #2 Information System
System Security Plan
Security Assessment Report
Plan of Action and Milestones
Security Information
System Security Plan
Security Assessment Report
Plan of Action and Milestones
Determine the risk to the first organization's operations and assets, individuals, other organizations, and the Nation and the acceptability of such risk.
Determine the risk to the second organization's operations and assets individuals, other organizations, and the Nation and the acceptability of such risk.

Figure 2-2. Building Trust Relationships Through Security Due Diligence

2.1.6 Information Security Governance

The ISE is fundamentally a joint mission capability requiring ongoing commitment by ISE participants and Implementation Agents[23] to exercise the actions necessary to accomplish the five foundations for trust discussed in section 2.1.5 above. The ISE governance structure will need to provide guidance, definition and oversight for the following:

- Actual categorization of ISE information. This includes definition of levels of impact of sharing/not sharing and guidance on determining impact levels by information type.
- Steps of the RMF (see section 2.1.1). Such guidance is expected to include ISE control baselines and ISE-specific guidance/restrictions to be applied for the tailoring of these baselines.
- Factors of trustworthiness (quality and assurance) needed to provide common starting points. Note that the ISE may provide guidance (or policy) on architectural issues/constraints necessary to achieve a level of trustworthiness.
- Cross-organization authorizations. This future guidance will also include relating emerging concepts of "data stewardship."
- Assessment of ISE systems, ongoing monitoring of these systems, and reporting of relevant status to ISE participants and Implementation Agents.
- Training requirements for personnel involved in the implementation and operation of the ISE.

[23] Further information regarding the use of ISE Implementation Agents can be found in Chapter 12 of the ISE Implementation Plan found at www.ise.gov, with detailed selection criteria and the process for selecting Implementation Agents will be documented in the ISE Enterprise Architecture Framework, Version 2.0.

- Processes and requirements for information sharing agreements.
- Establishing and maintaining ISE standards through CTISS.
- Resolving and dispositioning complaints regarding ISE improvements and revisions.

ISE governance processes should be incorporated into department/agency architecture and CPIC policies and processes. The ISE governance structure may require cooperative engagement through a governance body. This body could leverage existing governance structures, extending coverage to the broad range of ISE participants and Implementation Agents. Any governance body would need to be compatible with a diverse set of organizations and jurisdictions having no common authority. These organizations represent potentially different sharing perspectives despite having arrived at a set of common goals and objectives for information sharing. This governing body could provide assurance that information security safeguards and countermeasures are put in place to protect agencies' most critical assets.

2.1.6.1 Information Security Training Requirements

A lack of a uniform training program will lead to uncertainty about the way others handle and protect information, which in turn would undermine confidence and limit sharing. Trust between communities will require that participants have a common understanding of their responsibilities to both share and protect classified and controlled information. This trust will require establishment of mandatory information security training and certification and assistance. The most cost-effective information security training approach for building trust is to establish an ISE-wide training initiative that uses existing institutional frameworks and established curricula. The ISE should leverage, establish, and publish training guidelines, encompassing user and system administrator level training and sector specific training as well as data handling instructions for different categories of ISE data.

2.2 Information Flows

Information flows, derived from overarching ISE mission and service business processes, provide the interrelationships and interfaces between ISE participants for sharing information packages in the ISE. These flows provide the next level of detail from the business processes and provide key inputs into the information exchanges that provide the basis of CTISS functional standards. Information flows should identify the who, what, and where of products and technical and administrative formats and restrictions. The benefit of these information flows must also be consistent and mapped back to performance metrics of the ISE.[24] Information flows are expected to be inputs into the ISE EAF, with implementation guidance provided in the ISE PAIS.

[24] Performance metrics are documented in the Business Partition of the ISE EAF.

2.3 Enterprise Architecture

2.3.1 Conceptual Description

2.3.1.1 Service-Based Architecture

To promote the reuse of functional capabilities, the ISE is developing and implementing a service-based architecture approach. A service encapsulates business processes in the form of functional units. These units are combined to form composite applications that address complex business needs. Using ISE standards and ISE patterns, services can be developed using a variety of platforms while maintaining interoperability. The ISE EAF recognizes two primary service groups: legacy and contemporary.[25] Legacy services are those that are decomposed and exposed from already existing applications. By contrast, a contemporary service is developed specifically for use in the ISE.

Service-based architecture is developed iteratively, with each successive iteration providing greater functionality to the ISE Community of Interest (COI). In practice, the foundational services have long development life cycles. However, as additional services are built upon these foundational services and further composite applications are built leveraging services, the early investments yield large returns.

2.3.1.2 CTISS and Governance

To assure interoperability and successful information sharing, ISE participants are advised to adopt common standards. The CTISS Program[26] Issuances sets forth roles and responsibilities for the administration and implementation of CTISS issued by the PM-ISE. This issuance also assigns the ISC and the CTISS Committee, which reports to the ISC, as the administrative bodies for CTISS, responsible for establishing an integrated, nationwide enterprise of information sharing organizations and resources. CTISS defines two categories of standards:

- Functional Standards: Constitute detailed functional activity descriptions, data, and metadata on a focused area, such as Suspicious Activity Reports (SARs), that uses ISE business processes to share mission products.
- Technical Standards: Identify specific technical methods and techniques to implement information sharing capability into ISE participant systems.

Both functional standards and technical standards will be issued by the PM-ISE using the ISE issuance system.

[25] Program Manager, Information Sharing Environment, Information Sharing Environment Enterprise Architecture Framework, Version 1.0, found at Internet site http://www.ise.gov/docs/ISE-EAF_v1.0_20070830.pdf.

[26] The PM-ISE, using the ISE Issuance System, issued administrative memorandum, "ISE-AM-300 Information Sharing Environment Administrative Memoranda (ISE-AM) on the Common Terrorism Information Sharing Standards (CTISS) Program," found at Internet site http://www.ise.gov/docs/ctiss/ise-asm300-ctiss-issuance.pdf.

Additionally, the Information Sharing Environment, Information Assurance Working Group (IAWG) also defined IT security standards for the ISE fostering collaboration on the integration of IA and IT Security for the ISE environment. These standards will be issued through the CTISS as Technical Standards.

2.3.1.3 ISE Design Patterns

The Technical Partition of the ISE EAF describes the technologies, standards, and patterns used to implement the applications and services. Patterns are exemplar designs used to illustrate best practices when applying technologies and standards. Enterprise integration patterns represent industry best practices for describing a reusable design. In other words, patterns are a proven way to capture expert knowledge in fields where there are no simple, “one size fits all” answers, such as application architecture and integration.[27] The ISE EAF uses enterprise integration patterns to describe aspects of enterprise architecture integration that should be considered by agencies as they plan their participation in the ISE.

2.3.2 Implementer’s View

The Implementer’s View consists of the components shown in Figure 2-3. This view organizes the architecture artifacts into a model to guide participating organizations in the development of the ISE. Two segments are shown in the Implementer’s View: Core and Participant.

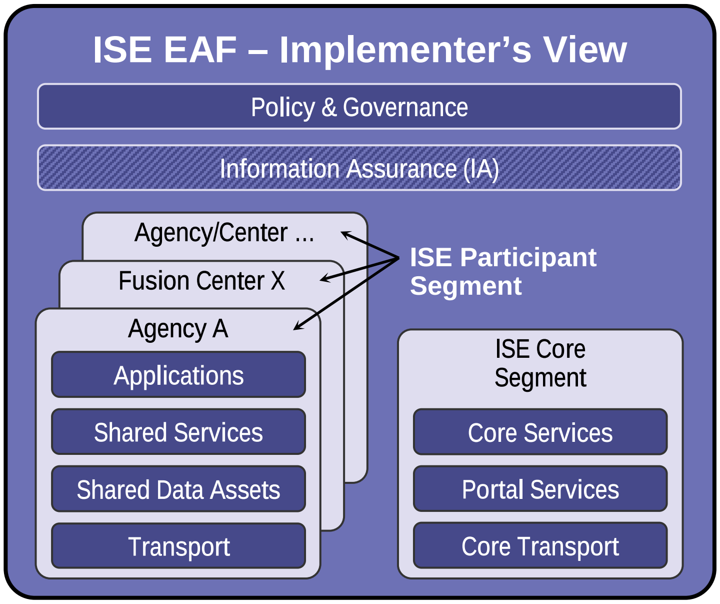


Figure 2-3. ISE EAF: Implementer’s View

[27] Program Manager, Information Sharing Environment, Information Sharing Environment Enterprise Architecture Framework, found at Internet site http://www.ise.gov/docs/ISE-EAF_v1.0_20070830.pdf.

2.3.2.1 Core Segment

The ISE Core Segment provides Core Services, Portal Services, and a Core Transport functionality to all participants in the ISE. The ISE Core is implemented as an extension of existing capabilities provided by an Implementation Agent for a given IT security domain (SBU, Secret, Top Secret/SCI).

- Core Services are required to provide a service-based architecture. These services provide common functionality used by all participants of the ISE.
- Portal Services support the ISE Portal and ISE Management Portal by providing services via user interfaces.
- Core Transport consists of the infrastructure and applications needed to support transmission and reception of services and information flowing through the ISE.

2.3.2.2 Participant Segment

The ISE Participant Segment illustrates shared services and components managed by participants and uses or provides information via the ISE. This document provides guidance on identifying, categorizing, developing, deploying, and maintaining these components. In addition, a foundational asset, transport, is inherently included in the Participant Segment.

- Applications provide capabilities to address the counterterrorism mission. They incorporate services and information through the ISE.
- Shared Services are provided by specific participants to address a business process. They provide access to data or capabilities from their particular organization.
- Shared Data Assets are information assets shared by participants via the ISE.
- Transport is a combination of infrastructure and applications providing information transmission between the participant and the ISE Core Transport.

2.3.2.3 Segment Architecture

Segment architecture refers to a business driven approach to defining and designing, in addition to other supporting architectural components, each participant’s ISE Shared Space.

As illustrated in Figure 2-3 above, the segment architecture describes each participant’s approach to the business processes and shareable assets in the Participant Segment.

Prior to developing solution architectures, the segment architecture should be well defined and accepted. As it relates to the ISE, the segment architecture is also a fundamental building block to developing an ISE Shared Space.

2.3.2.4 Solution Architecture

Solution architecture refers to a business driven approach to developing shareable assets and IT components in support of business processes identified in the ISE EAF and Participant Segment architecture. Solution architecture describes the process of developing individual shareable assets for use and integration into the segment architecture. Prior to developing solution architectures, the segment architecture should be well defined because it provides the framework around which each solution is created.

2.3.3 ISE Shared Space

The ISE Shared Space denotes infrastructure where segment and solution architectures are implemented leveraging CTISS and where each ISE participant makes terrorism information accessible to the ISE community. This infrastructure remains outside an ISE participant's internal network yet is under the management and control of that ISE participant.

To illustrate the ISE Shared Space concept, consider on-line stores or vendors. In this scenario they collect information such as name, contact information, credit card information, etc., stored in a database. Likewise, assets such as search and shopping cart services, along with an inventory are stored within the same network. The services and inventory represent the components of the store's shared space, available to the community to access and leverage based on their identity and credentials. The personal identification information is stored securely on the same network but is not in the shared space, and therefore inaccessible by the community. The ISE Shared Space functions in the same fashion, allowing for selective exposure of information and services with a terrorism nexus.

Chapter 3 – ISE Architecture Implementation Life Cycle

3.1 Introduction

The ISE enables participants to share terrorism information more effectively and efficiently. The Information Sharing Environment Architecture Implementation Life Cycle (ISEA ILC) presents a six-stage process following the guidance found in the ISE Enterprise Architecture Framework[28] to develop and implement an information sharing segment architecture and an ISE Shared Space. Each stage is completed collaboratively in support of cross-agency "To-Be" mission business processes. This approach promotes reuse of shareable assets across agencies rather than stove-piped development.

The term "life cycle" refers to a continuous iterative process that ISE participants and Implementation Agents should follow in implementing their capability to interface with the ISE. Over time, as the ISE evolves and matures, these iterations will occur with less frequency. Figure 3-1, below, illustrates the ISEA ILC.

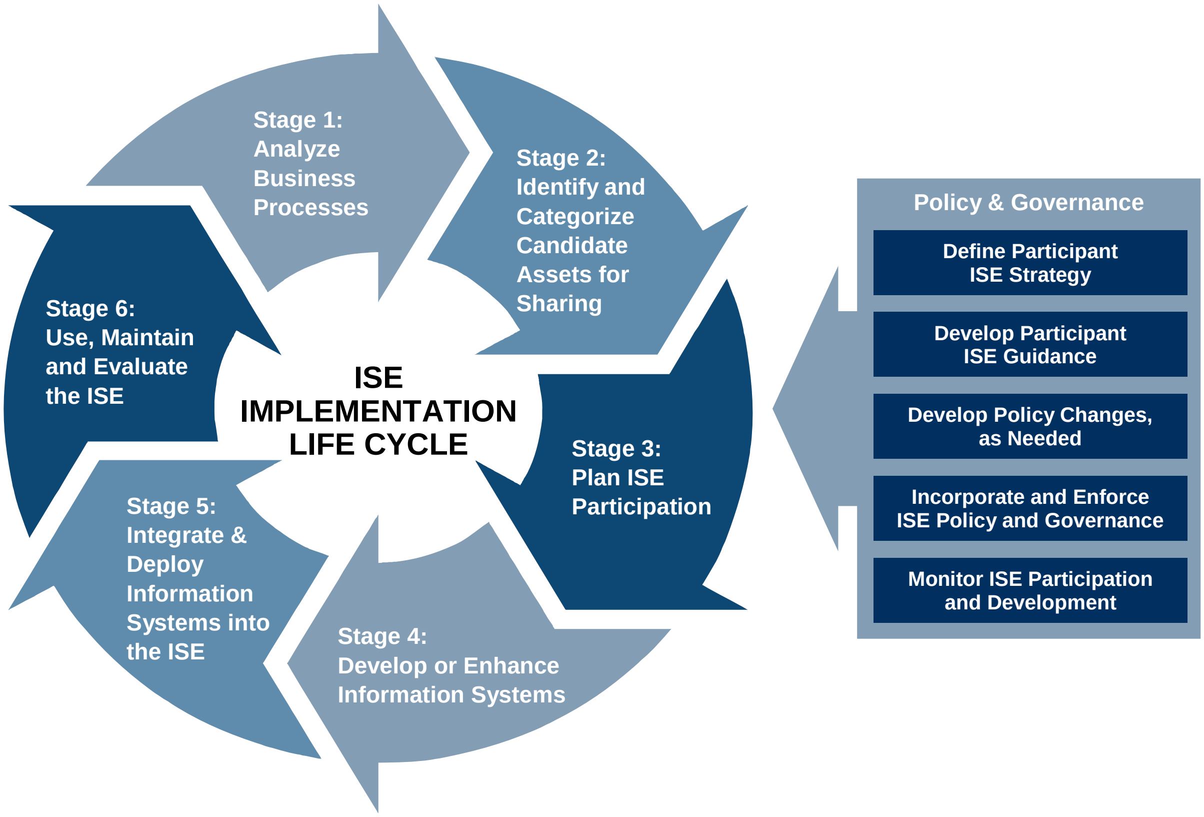

Stage 1: Analyze Business Processes
Stage 2: Identify and Categorize Candidate Assets for Sharing
Stage 3: Plan ISE Participation
Stage 4: Develop or Enhance Information Systems
Stage 5: Integrate & Deploy Information Systems into the ISE
Stage 6: Use, Maintain and Evaluate the ISE
ISE IMPLEMENTATION LIFE CYCLE
Policy & Governance
Define Participant ISE Strategy
Develop Participant ISE Guidance
Develop Policy Changes, as Needed
Incorporate and Enforce ISE Policy and Governance
Monitor ISE Participation and Development

Figure 3-1. ISE Architecture Implementation Life Cycle

[28] Program Manager, Information Sharing Environment, Information Sharing Environment Enterprise Architecture Framework, found at Internet site http://www.ise.gov/docs/ISE-EAF_v1.0_20070830.pdf.

The ISEA ILC encompasses the business processes, information flows, and information system(s) development, improvement, and deployment that enable participation in the ISE. Each stage is influenced or driven by policy and governance components, including strategy provision, guidance, policy updates, and monitoring functions to support progressive leveraging of the ISE. Each iteration of the life cycle plays an integral role in enterprise architecture and CPIC activities performed by each participant in accordance with OMB guidance.[29] Courses of action and governance should be implemented in accordance with the ISE Issuance System.[30]

From Figure 3-1, in order to successfully participate in the ISE, the following iterative process is recommended. Each stage includes a description of the way the stage contributes to the establishment and maintenance of trust among ISE participants and Implementation Agents as well as the applicable step(s) from the ISE RMF that are applied during each stage.

1. In Stage One, ISE participants and Implementation Agents should analyze their business processes and establish the ISE common risk management governance process to balance the access of information with risks among all Federal, SLT, and allied participants. This is a concerted, collaborative cross-agency effort to analyze the mission business processes. There are multiple desired outcomes of this business process analysis: First, identification and understanding of the current "As-Is" business processes. Second, identification of explicit goals and objectives for participation in the ISE. Third, determination of what modifications should be made to achieve target "To-Be" processes that take advantage of ISE-provided information.

   Foundation for trust in Stage One: Identification of common goals and objectives for sharing information.

2. In Stage Two, ISE participants and Implementation Agents identify and categorize candidate assets[31] for sharing. The desired output from this stage is a collection of assets, expertise, and current capabilities, which are appropriate for inclusion in the ISE. Categorization of these assets with regard to sharing/non-sharing impacts, determination of the resulting risks, and regulatory and statutory sharing restrictions provides this output. This stage is not dependent on any other stages and can begin immediately.

   Foundations for trust in Stage Two: Identification and agreement upon the risk associated with the information sharing activities.

   Associated Risk Management Framework step: Categorize information and information system(s).

[29] A detailed treatment of Section 53 filings can be found at Internet site http://www.whitehouse.gov/omb/circulars/a11/current_year/s53.pdf.

[30] Office of the PM-ISE, Information Sharing Environment Implementation Plan, November 2006, found at Internet site http://www.ise.gov.

[31] In this context, "counterterrorism asset" includes data, information, services, systems, networks, or other components to support the counterterrorism mission.

3. In Stage Three, ISE participants in conjunction with Implementation Agents plan for participation in the ISE, engineering the business processes and information flows identified in Stage Two. While policy and governance is intertwined throughout this entire ISE ILC, the policy and governance oversight is called out specifically in this step. A successful plan to participate requires the designated Implementation Agent and the ISE participant to work together to ensure implementation complies with overarching ISC policy and governance structures. Once business process analysis is complete, participants should develop a migration plan that transitions use of “As-Is” business processes, information flows, and technology to “To-Be” versions consistent with those documented in the ISE EAF and other documents. As an integral part of this planning, they identify the required level of system trustworthiness, including regulatory/statutory restrictions on information sharing and special handling procedures, to adequately address the risks determined in the previous stage and define the requirements necessary to achieve this trustworthiness.

   Foundations for trust in Stage Three: An agreed scope of trustworthiness needed for the ISE information system(s) processing, storing, or transmitting shared information in order to adequately mitigate the risk.

   Associated Risk Management Framework step: Select, Supplement, and Document Security Controls.

4. In Stage Four, ISE participants and Implementation Agents develop or enhance their IT components. To the extent possible, existing IT components should be enhanced and leveraged. If existing IT components are not sufficient, new components should be acquired to accomplish information sharing objectives identified in Stages One and Three.

   Associated Risk Management Framework step: Implement Security Controls.

5. In Stage Five, ISE participants and Implementation Agents integrate and deploy IT components into the ISE. This stage constitutes implementation of the modified business processes, information flows, and enhanced IT components within the ISE constructs. This stage also includes verification that ISE requirements have been met and the explicit risk decision made whether to authorize participation in the ISE.

   Foundations for trust in Stage Five: Determining if the respective implementations of the ISE information system(s) are worthy of being trusted to operate within the agreed-upon levels of risk despite environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation.

   Associated Risk Management Framework steps: Assess Security Controls and Authorize Operation.

6. In Stage Six, ISE participants and Implementation Agents operate and maintain their systems supporting the ISE. ISE capabilities should be assimilated into routine participant processes. Successful participation is also dependent on

sufficient staff training and identification of enhancement opportunities in addition to operation and maintenance activities. Identification of enhancements and new data sources leads into a subsequent iteration of the ISE life cycle. Stage Six is a continuous process until Stage Five of a subsequent iteration is complete.

Foundations for trust in Stage Six: Providing ongoing monitoring and oversight to ensure that the ISE trust relationship is being maintained.

Risk Management Framework step: Monitor security controls (and operational environment).

Each participant assesses existing policies and governance mechanisms in light of the desired information sharing environment. The participant's strategy to participate in the ISE should steer the development of specific guidance to reengineering business processes, information flows, planning, information system(s), and operational activities. Issuances may need to be developed and disseminated for any guidance around revised processes and /or technology guidance. Each participant will incorporate ISE guidance into routine operations and enforce compliance. Feedback and involvement from mission users and information system(s) managers are necessary to ensure that ISE solutions add value to the counterterrorism mission. Individual ISE implementation efforts to meet specified capability requirements will need to be coordinated among ISE participants, including Implementation Agents. Each stage is described in further detail in the following sections.

3.2 Stage One: Assess Existing ISE Mission Business Processes and Performance Characteristics (Assess and Validate the Performance Reference Model Goals and Target)

3.2.1 Description

The first stage in building and designing enterprise, segment, and solution architectures (and the organization's ISE implementation approach) is to explicitly determine mission critical business objectives, performance outcomes, and needs. Within this stage, ISE participants assess current business processes, practices, policies, and rules to achieve measurable, implementable, and realistic outcomes as governed by either PM-ISE performance metrics, which influence OMB EA Budget Plans, or other PM-ISE issuances. This stage is tightly coupled with Stage Two, "Identify and Categorize Candidate Assets for Sharing." Stages One and Two can be undertaken simultaneously or sequentially. An organization's team that supports these stages overlaps to include representatives from each community, business process experts, information assurance and Policy specialists, IT experts, the enterprise architects (in most cases the Chief Architect), and resource planners. Coordination with external stakeholders occurs via community representatives, ISE Implementation Agents, and external agency IT contacts. The assessment team should coordinate with internal users, portfolio managers, and operations support staff.

All subsequent activities and stages are driven and influenced directly by assessing current business processes from supporting the intra-agency "To-Be" ISE Mission Processes and aligning ISE mission performance metrics to validate determined goals and targets.

3.2.2 Activities

3.2.2.1 Information Security

In this stage ISE participants and Implementation Agents identify and make explicit for others to see the goals and objectives each organization participating in the ISE has for the information sharing to be conducted. These goals and objectives drive the decisions made in the other stages of the ISE implementation life cycle. In addition the ISE common risk management process will take the ISE participants' and Implementation Agents' goals and objectives and integrate them to determine the "To-Be" actions required to maximize information sharing.

3.2.2.2 Architecture Analysis

The business requirements for each ISE participant and Implementation Agent need to be determined by reviewing their "As-Is" business processes along with the notion of where they need to go, taking advantage of other participants' information. Based upon this analysis, the functional and technical requirements for the supporting CTISS can be developed. Before identifying the business processes required for successful transition into the ISE, requirements analysis must be completed. The analysis yields a matrix of derived technical requirements pertaining to the hardware, software, and transport capabilities required to begin design of the solution architecture. This analysis also feeds into the testing and evaluation of each IT component as it relates to participation in the ISE.

To perform functional requirement analysis, ISE participants should use the following high-level procedure:

1. Develop use cases mapped to functional requirements.
2. Identify business processes required to perform each use case, including the handling of special categories of information, as required by regulation or statute.
3. Identify shareable assets required to support the business processes.
4. Develop solution architectures in alignment with the segment architecture and functional requirements.
5. Identify the data handling requirements and sharing restrictions (if any) mandated by regulation, statute, or prior agreement with stakeholders.

Each ISE participant should support the ISE business process analysis to determine whether mission assets can be modified to take advantage of the ISE-provided mission information. Successful business process reengineering (BPR) involves agency-wide commitment and careful analysis of the "As-Is" environment to discover ways to improve, modernize, enhance, or remove inhibitors that prevent forward progress toward a robust "To-Be" infrastructure.

As referenced within the ISE EAF, the National Information Exchange Model (NIEM) Concept of Operations highlights a Department of Justice scenario analysis that helps put in a realistic scenario of what must occur for the agency to achieve its mission goals and objectives. This scenario analysis can be technology independent, which could then align to the ISE participant's segment EA analysis.

As potential business processes, information flows, practices, or rules are analyzed, related policy changes may also be identified. This process directly aligns with Stage Two, which examines the need to prepare a Gap Analysis Assessment. Implementation Agents and ISE participants (to include intra-agency/cross-agency considerations) must evaluate and identify areas for improvement, based on possible ineffective, unused, or rigid processes that do not lend to enabling a true ISE.

Some questions that must be answered by ISE Implementation Agents and/or ISE participants that are defining mission needs should include the following:

1. What are the National Intelligence Sharing requirements?
2. What information will be shared based on CTISS functional standards and other guidance?
3. Is the right information being shared today? Why or why not?
4. What is the intended use of the information?
5. What mission processes are being supported?
6. Who has the data needed to share, or who has previously unknown terrorist information that could augment existing data?
7. How is data accessed?
8. Who/where are the authoritative sources of data usage and interpretation?
9. What are the risks or the consequences if sharing does not take place?
10. What is the business process to achieve the level of trust (risk mitigation/management) to assess the security protections used within the ISE?[32]
11. Where are the gaps? (e.g., pain points)
12. What policies need to be revised to enable and make for an effective ISE?

[32] Section 1016 of IRTPA.

13. What is the mission risk of not having access to the information? Is that a managed risk or risk avoided?
14. How has the unanticipated user risk been mitigated?
15. Who are our exchange partners?
16. In what form is our organization required to share information today?

Throughout this process, the ISE participant monitors other ISE-related activities to stay abreast of what capabilities are planned or already available.

3.2.3 Implementation Agent Considerations

This stage sets the overall tone and direction for the degree of effectiveness of the ISE. ISE Implementation Agents, along with the ISC, must collaborate and coordinate with inter-organizational and intra-organizational ISE participant representatives to address and resolve the questions above to determine the existing landscape of the organization and a realistic approach to remove potential cultural, technological, political, security, social, or technological barriers or inhibitors in order to support true information sharing based on mission needs. Once the data is discoverable and the data is correlated, the Implementation Agent will assist ISE participants in binning the data to increase the quality and enhance the flow of information/exchanges.

3.2.4 Outputs/Outcomes

Output: The desirable outputs for this stage are not only essential inputs for the next planning stage; they are also building blocks for which the other stages are designed, governed, and implemented. These fundamental stages lead to an achievable "To-Be" process that takes advantage of ISE-provided mission asset information. The results of this stage include use cases,[33] business process models,[34] and information flow descriptions[35] that are part of each revised business/mission process description. Along with the "To-Be" cross-agency business process, another desired output would include a roadmap that illustrates the transition from "As-Is" to "To-Be" processes and appropriate traceability to applicable policies to assist in a successful implementation of Stages Two through Six. In addition, the ISE will have established a common risk

[33] Use case diagrams represent high-level business process scenarios. Use cases identify the major processes, describe the actors (people or organizations) involved, and identify the interaction between the actors and the processes.

[34] The business process models provide additional detail to the information flows for an actual ISE business process. Each event, activity, responsible party, and interactions can be described for a set of terrorism information sharing business processes. Boundaries and responsibilities within and between participating organizations can also be highlighted.

[35] Information flows are characterized so that specific data elements that are being shared or should be shared can be identified. The information flows are used to develop a high-level model and a vocabulary to represent the information exchanges. Another perspective countering the outcomes of this step is to actively review business processes, practices, and rules that could benefit from the ISE and develop (or modify) use cases, a business process model, and a description of relevant information flows.

management governance process to address the difference in risk management issues between the ISE participants and Implementation Agents.

Outcomes: The PM-ISE, along with ISE Implementation Agents and ISE participants, have analyzed, assessed, and modified existing business/mission processes to enable/allow the active movement of data to traverse organizational, cultural, technological, and policy boundaries to promote the sharing of relevant data and other critical assets and resources.

A mutually agreed-upon (organization/ISE and/or organization/organization) set of information sharing goals and objectives that forms an effective definition of the purpose for ISE participation and adequately defines the organization's intent for the purpose of driving information system(s) security decisions.

3.3 Stage Two: Identify and Categorize Candidate Assets for Sharing

3.3.1 Description

In building an ISE Shared Space within enterprise, segment, and solution architectures, each ISE participant determines the organization's shareable counterterrorism assets.[36] Likewise, each ISE participant identifies what gaps exist in current asset inventories. This analysis identifies what components of the enterprise, segment, and solution architectures are in place, and further, what components are needed to achieve the "To-Be" state. Each data, service, and application asset maps to information sharing segment architectures addressing the data and application and service layers. Each asset should directly support or address the business processes addressed in the previous stage.

During this stage an ISE participant and Implementation Agent develops a thorough understanding of the assets available for exposure via the ISE based on the outputs of Stage One. This analysis is composed of building an asset inventory and identifying gaps that hinder the "As-Is" business processes from supporting cross-agency "To-Be" mission business processes. The key artifacts created during this activity are the asset inventory and the asset gap analysis. This stage provides input into the Performance, Business, Data, Application and Service, and Technical layers of an ISE participant's segment and solution architecture.

Additionally, during this stage the potential risk and impact of sharing and of not sharing are determined.

[36] Assets are defined as the data, services, and applications within an organization's infrastructure.

3.3.2 Activities

3.3.2.1 Information Security

During this stage an ISE participant and Implementation Agent develops a thorough understanding of the data, service, capabilities, subject matter expertise, and application assets available for exposure via the ISE based on the outputs of Stage One. The assets identified for sharing are categorized in accordance with ISE policy and guidance regarding potential impacts upon the organization, individuals, other organizations, and the Nation both from the perspective of what may occur if the information is shared and what may occur if the information is not shared. Additionally, this categorization is used in making explicit determination of the risks being incurred, including the limitations by regulation, statute, or prior stakeholder agreement on whether and how the information is shared.

Key questions posed during this stage include

- What is the risk if this information is shared?
- What is the risk incurred if this information is not shared?

3.3.2.2 Architecture

In identifying their assets, ISE participants and Implementation Agents create an asset inventory. The goal of an asset inventory is to identify the counterterrorism assets already positioned within an ISE participant. Each inventory consists of data, service, and application assets. Assets selected for this inventory directly support and affect cross-agency capability to effectively share information. Assets that do not support the cross-agency “To-Be” processes should not be included in this inventory. Typically, services and applications selected for sharing in this process support or give access to the identified data assets. When considering an asset for the counterterrorism mission, each ISE participant should consider whether that asset is

- Highly valuable to other ISE participants’ counterterrorism missions as evident in the cross-agency “To-Be” mission process determined in Stage One
- Sufficiently documented and interpreted
- Related to any of the identified ISE business processes
- High quality
- Available for timely provision
- Service-based architecture ready
- Permissible to share and use under national security, legal and internal considerations, privacy policies, and restrictions mandated by regulation or statute
- Available for timely, cogent, and complete provision

In addition, each asset has specific requirements to consider when it is identified for sharing via the ISE.

Data assets are stored, accessed, and retrieved within ISE Shared Spaces using metadata and transferred across or within the five ISE communities'[37] Shared Spaces using information exchanges as defined by CTISS functional standards. If an information exchange does not exist for a targeted data asset, it must be developed and made available for participants via the ISE Portal. Service and application assets are described using Description Documents and Service Level Agreements (SLA).

To create an asset inventory, ISE participants should use the following high-level procedures:

1. Identify and categorize data assets for sharing, including system and data owners.
2. Align data assets with identified business processes in segment architectures.
3. Identify information exchanges for each data asset to be shared.[38]
4. Identify and categorize service assets for sharing.
5. Create service descriptions.[39]
6. Identify and categorize application assets for sharing.
7. Create application description.
8. Leverage existing documentation (information exchange package documentation, description, SLA) rather than recreate additional documentation.
9. Append known information on security restrictions and information handling instructions.

Understanding what assets an ISE participant does not govern is equally important as knowing what a participant does govern. The identification of these gaps is discovered by performing an asset gap analysis. Asset gap analysis is performed to identify the assets that would improve the business processes of the ISE participant. This analysis, with the knowledge of what potential assets are available through the cross-agency "To-Be" mission analysis, should be conducted in close collaboration with business process analysis.

When "pain points" or hindrances in existing business processes are identified, there are two solutions: Either the process must change, or the resources must be improved.

[37] The five communities as defined by the ISE Implementation Plan are Intelligence, Law Enforcement, Defense, Homeland Security, and Foreign Affairs.

[38] The IEPD Clearinghouse provides a broad variety of information on IEPDs. This source includes examples that have been submitted by individuals and organizations who have implemented the Global Justice XML Data Model (Global JXDM) and the National Information Exchange Model (NIEM). These examples can be found at Internet site http://www.it.ojp.gov/iepd/.

[39] The standards for providing Web service descriptions is maintained by the World Wide Web Consortium (W3C). Documentation for this standard can be found at Internet site http://www.w3.org/TR/ws-desc-reqs/.

This analysis aims to lay the foundation for the latter. By identifying assets to improve the business process, the ISE participant is better prepared to meet mission goals. The resulting analysis will help a participant determine what areas of the enterprise and segment architecture need fortification.

To create an asset gap analysis, ISE participants should use the following high-level procedures:

1. Leverage business process analysis to identify asset gaps.
2. Identify gap data and application and service layers of segment architecture.
3. Identify and categorize asset types required (data, service, or application).
4. Coordinate SLAs with Implementation Agents for service and application assets.

Using this analysis, ISE participants can query asset registries on the ISE to fill the gaps in their architectures and create a more complete, robust process in addressing the mission.

3.3.3 Implementation Agent Considerations

Given that this step could be executed in tandem with Stage One, this step is equally important. The ISE Implementation Agent will engage ISE participants to identify and categorize mission assets after reaching a common understanding of mission direction and intent for the ISE. Much of categorization within this stage will be derived from questions including, “What is the risk of sharing vs. what is the risk of not sharing?” and “What mission processes are being supported based on need to provide mission assets in a timely and secure fashion?”

It is understood that, in certain environments, the perception of releasing all information could have severe impact to the Nation’s security. A solution to this concern is to appropriately use metadata tagging standards and dissemination/release controls and handling instruction to ensure the integrity of the data is not compromised. Here the ISE Implementation Agent must be keenly aware of identification, security controls, and categorizations that have been put in place to assist in this process.

3.3.4 Outputs/Outcomes

Output: The specific output of this stage is a well-defined segment architecture. It provides the “As-Is” and “To-Be” views of information sharing. The segment architecture is used to build specific business cases to justify funding for transitioning into the ISE. For each shareable asset identified during the inventory, analysis and solution architectures are created. In the subsequent stage, the steps to build the business case for each solution are provided.

Outcomes: The desired outcomes for this stage are

- All essential inputs from the next stage are available in a form suitable for use with sufficient content and accuracy
- A mutually agreed-upon definition of the risks being incurred by the intended participation in ISE as well as the expected benefits of that participation
- Agreement by all affected authorizing officials with the definition of risks to be incurred

3.4 Stage Three: Plan Transition to Information Sharing Environment

3.4.1 Description

Once business process analysis and an asset inventory are created, each ISE participant formulates a strategy and implements a solution architecture to support the processes of the agency segment architecture. This strategy continues to build on the analysis performed in each of the previous stages. Using the gap analysis and current asset inventory, new development and enhancement of data, service, and application assets can be targeted. During this stage the business case, as required, and alternatives analysis are performed. Additionally, this stage includes defining the level of trustworthiness needed for the ISE information system(s) involved and detailing the requirements necessary to meet this level of trustworthiness. This artifact will also aid in formulating participating agencies' Section 300 – Information Technology and E-Government investment plans with regard to enterprise architecture and resulting segment architectures.[40]

3.4.2 Activities

3.4.2.1 Information Security

As cited in Chapter 2, applicable ISE policy and guidance, as well as applicable regulation or statute, is applied in determining the degree of risk mitigation needed within the associated ISE information system(s). This assessment translates into a level of trustworthiness needed and hence into a set of requirements for functionality, quality, and assurance. The specific requirements to be applied are determined by applying the process described in NIST Special Publication 800-53, using ISE-specific control baselines and additional tailoring guidance/constraints along with the determination of level of trustworthiness to be obtained.

[40] A detailed treatment of Section 53 filings can be found at Internet site http://www.whitehouse.gov/omb/circulars/a11/current_year/s300.pdf.

3.4.2.2 Architecture

A business case and alternatives analysis provide strategy and rationale for investing in, developing, and enhancing shareable assets in support of the ISE and agency segment architectures. During this activity several key artifacts are created including alternatives analysis, recommended solutions, level of effort estimate, and rough order of magnitude. The business case's sole objective is to demonstrate the value of investing in the segment and supporting solution architecture in support of the cross-agency mission processes.

ISE participants should use the following procedure to develop the business case for investments in their segment architecture:

1. Prepare summary information about the ISE investments required for transitioning to the ISE. Include descriptions of each proposed shareable asset and the way they close identified performance gaps (identified through Stages One and Two).
2. Identify whether ISE investments are included in the agency's target EA, EA transition strategy, and existing segment architecture. If it is not included in any of these, prepare documentation to justify its exclusion.
3. Create descriptions that summarize the purpose and business processes of assets and their alignment with the ISE EAF and FEA Consolidated Reference Model.
4. Perform an alternatives analysis for each solution. Evaluate whether custom development is required or commercial off-the-shelf (COTS) or Government off-the-shelf (GOTS) solutions are available to support the needs of the segment architecture. During this process, include documentation justifying why each alternative was selected.
5. Ensure that risk management strategy for each investment aligns with the Risk Management Framework presented in Chapter 2 of this document.
6. Create a work breakdown structure for development of the segment architecture including an estimated level of effort and the rough order of magnitude for the development, deployment, operation, and maintenance of each shareable asset.
7. Prepare quantitative performance metrics for each shareable asset to measure the improvement in cross-agency capability. ISE baseline measures include Federal, State, local, tribal, and foreign partners information needs;[41] creating a culture of sharing; common security framework; and architecture and standards. These metrics are also included in the OMB Federal Transition Framework Catalog.

[41] Portions of the baseline measure category only apply to DHS, DoJ, FBI, and NCTC.

Once this activity is complete, each participant should have a fair estimate of the investment and accompanying justification needed to develop and enhance assets in alignment with enterprise and segment architectures for participation in the ISE.

Leveraging the outputs of the process described above, each agency can develop its IT Investment plans regarding enterprise architectures as instructed in Section 300 of OMB Circular No. A-11, entitled Preparation, Submission and Execution of the Budget.[42]

3.4.3 Implementation Agent Consideration

During Stage Three, in creating a roadmap to illustrate the steps and estimated level of effort for each, ISE participants must collaborate with ISE Implementation Agents. This collaboration is necessary to ensure that shareable assets are integrated into the ISE Core and Portal. Additionally, the internal agency transport must have the ability to connect to the ISE Core Transport. In order to plan for this level of integration, all Core Service, Portal Service, or Core Transport Implementation Agents must provide the necessary documentation and descriptions of their provided service.

3.4.4 Outputs/Outcomes

Outputs: In this stage, leveraging the outputs of Stages One and Two, a business case and alternatives analysis provide direct input into the CPIC processes regarding the OMB Circular No. A-11, Section 300,[43] IT Investments for each solution architecture.

Outcomes: The desired outcomes for this stage are

- All essential inputs for the next stage are available in a form suitable for use with sufficient content and accuracy
- A mutually agreed-upon definition of the trustworthiness to be achieved in the associated ISE information system(s)
- A mutually agreed-upon set of information system(s) requirements for security functionality, quality, and assurance
- Agreement by all affected authorizing officials with the defined trustworthiness level and related information system(s) requirements

[42] A detailed treatment of Section 53 filings can be found at Internet site http://www.whitehouse.gov/omb/circulars/a11/current_year/s300.pdf.

[43] Ibid.

3.5 Stage Four: Develop and Enhance Information Technology Components

3.5.1 Description

Once business process analysis and asset inventories are created, each ISE participant can begin to develop and enhance IT components to meet requirements and address gaps identified in the previous stages in conjunction with Implementation Agents' schedules. During this stage, each ISE participant leverages its internal development procedures, while augmenting several ISE development practices to develop and enhance assets and components in support of segment and solution architectures.

To the extent possible, existing assets should be used not only to reduce cost but also to promote reuse. Where gaps exist that cannot be filled with existing or enhanced components, new components should be developed. Each IT component must accommodate information security requirements and adhere to ISE technology standards and patterns.

Each component developed should directly support data, service, and application assets identified during the business process analysis and asset inventory stages as well as map to the participant's segment architecture.

3.5.2 Activities

3.5.2.1 Information Security

The information system(s) security requirements identified in the previous stages (functionality, quality, and assurance) are implemented.

3.5.2.2 Activities

Using functional requirements, technical requirements, and solutions architecture, an agency can create a requirements traceability matrix. This matrix, as development progresses, will map development directly to the functional requirements and business processes. This unique mapping enables easier testing and verification of functionality.

To develop new IT components, ISE participants should use the following high-level procedures:

1. Use the participant- specific development cycle to design and develop IT components, taking into consideration the outputs of Stages One and Two.
2. Augment internal design artifacts with service or application specifications that instruct other ISE participants on procedures to leverage IT components and the way they map to their enterprise architecture, including markings and handling instructions.

3. Create and execute IT component unit and integration test cases.
4. Update and enhance information exchanges to accommodate changes made during the development cycle.
5. Update and enhance SLA to accommodate changes made during the development cycle.
6. Update information exchange schemas, service descriptions, and standards in ISE asset registry.
7. Develop standards-based translation services to enable inflow and outflow of data for each legacy component being leveraged.
8. Develop User Access Controls, as required, based on information restrictions and handling instructions.

As ISE participants develop shared IT components, the need to develop new components will reduce, promoting greater asset reuse and information sharing. This is the foundation of using a service-based architecture. As more services become available, the ability to create composite applications to leverage assets in support of the enterprise and segment architecture becomes easier and more cost efficient.

3.5.3 Implementation Agent Considerations

Each data, service, or application asset developed for the ISE must also be compatible with the ISE Core and Portal. In order to develop the necessary protocols, each agency leverages design guidance to be provided by each ISE Implementation Agent. This guidance provides detailed descriptions and procedures to ensure compatibility and connectivity to the ISE Core and Portal.

3.5.4 Outputs/Outcomes

Outputs: Stage Four yields System Design Life Cycle (SDLC) documentation as specified by each individual agency.

Outcomes: The desired outcomes for this stage are

- All essential inputs for the next stage are available in a form suitable for use with sufficient content and accuracy
- The information system(s), as implemented, fully complies with the defined information system(s) security requirements for functionality, quality, and assurance

3.6 Stage Five: Integrate Information Technology Components into the ISE

3.6.1 Description

ISE participants and Implementation Agents integrate newly developed and enhanced IT components into their ISE Shared Spaces. The process begins with establishing the assets as configuration items in the ISE test and evaluation environment. Next, shared data are exposed, shared services are registered, and applications are hosted in the ISE test environment. The assets can then be tested in the ISE test and evaluation environment to ensure that they are accessible and perform as intended.

3.6.2 Activities

3.6.2.1 Information Security

An assurance case is developed for the ISE information system(s) that combines information from the specification, design, development, and implementation from previous stages with assessments performed in this stage, documenting the grounds for confidence that intended functionality has been implemented with the required level of quality. Assessments are performed in this stage, to the degree necessary, to complement the other evidence from previous stages in achieving the required level of assurance. PM-ISE provides guidance and oversight of the assessment as necessary to facilitate and maintain trust among those participating in the ISE that agreed-upon levels of trustworthiness have been achieved.

3.6.2.2 Architecture

The first activity in this stage focuses on preparing and executing component deployment into the ISE Test & Evaluation environment for user acceptance and integration testing. Additionally, performance and load testing are completed during this stage.

In order to deploy IT components into the ISE, a deployment plan is created. This plan includes all the assets required for integration, a step-by-step deployment script, and initial configuration management steps.

In addition to preparing the component for deployment, the necessary training documentation is created for delivery with the actual solution. Training is necessary and provides users with the correct data, service, and application usage guidance. It is essential that a training environment for shareable assets is made available in order to avoid impeding development, testing, and evaluation.

ISE participants should use the following high-level procedures to develop a deployment plan:

1. Prepare deployment scripts to expose data assets for sharing, register service assets using CTISS for the ISE, and install and host application assets on the ISE.
2. Apply configuration management tools to control deployed assets.
3. Prepare user acceptance, performance, and load testing scripts for use in the ISE test and evaluation environment.
4. Prepare concept of operations and user manual documents to supplement new and enhanced IT components in support of shared assets.
5. Prepare insertion packages for new components and services to be inserted into an ISE participant's enterprise architecture.
6. Prepare training documentation and delivery mechanisms for user indoctrination once deployment commences.
7. Develop a communication plan aligned with identified system, application, or service stakeholders. The plan should define the deployment and training plans and provide a mechanism for user feedback.
8. Develop user training for handling restricted categories of data as applicable.

Once completed, this activity results in successful deployment of the shared assets identified during business process and asset inventory analysis. Deployed assets should address gaps identified during this analysis. In addition, new assets are now part of the segment architecture and align with the enterprise architecture.

During the deployment stage several types of testing must be conducted. Unit and integration testing should have been completed during the development stage. During deployment, user acceptance, performance, and load testing are conducted. These activities are performed in the ISE test and evaluation environment described in Section 1.4 of this document. This evaluation is critical because it validates the effectiveness or business rules and performance measurements to ensure that the technology solutions accurately provide impact desired for the ISE.

The following high-level steps provide guidance on testing assets to be deployed:

1. Perform user acceptance testing, using a group of end-users, once deployed to the test and evaluation environment.
2. Conduct performance and load testing to ensure reliability of the systems during high information traffic.
3. Collect test results; remediate and retest if required.

Once testing is complete, the requirements traceability matrix can be completed as well. This matrix provides a requirement for capability mapping that illustrates all functional requirements have been addressed during the process of development and deployment of data, service, and application assets.

3.6.3 Implementation Agent Considerations

This is the stage (Stage Five) at which ISE Implementation Agents will actually deploy the service or core capabilities for which they are responsible. In many cases, this means that the Implementation Agent will execute a rolling deployment – led by a pilot roll-out, followed by an initial roll-out, followed by a general roll-out, and finally entering a maintenance phase in which new features/versions and customers are added and rolled-out periodically. Typically, this strategy means that the Implementation Agent will begin by preparing a detailed roll-out plan and schedule, and this plan and schedule will be coordinated with other ISE participants who are directly affected.

3.6.4 Outputs/Outcomes

Outputs: Stage Five yields the necessary deployment documentation for each shareable asset including configuration documentation and training documentation. Additionally, the final testing results are compiled.

Outcomes: The desired outcomes for this stage are

- All essential inputs for the next stage are available in a form suitable for use with sufficient content and accuracy
- An assurance case exists that provides all necessary information, in a form and presentation that facilitates effective use, to enable agreement among all affected authorizing officials that the intended information system(s) security functionality has been implemented with the required degree of quality
- All affected authorizing officials approve the operation of the ISE information system(s) for the intended information sharing and the accomplishment of sharing goals and objectives identified in Stage One

3.7 Stage Six: Operate, Maintain, and Evaluate the ISE

3.7.1 Description

The final stage in the ISE Architecture Implementation Life Cycle addresses operation, maintenance, and evaluation of the ISE. During this phase, ISE shared assets and tools are integrated into the day-to-day activity of participating organizations. Additionally, shared assets are monitored and maintained to ensure the reliability of information and services leveraged via the ISE. Finally, shared components and use of the ISE are evaluated using performance metrics. Identifying gaps in performance will enable the discovery of new areas to address in the next iteration of the ISE Architecture Implementation Life Cycle.

3.7.2 Activities

3.7.2.1 Information Security

This stage accomplishes the fifth foundation for trust: ongoing monitoring and oversight to ensure that the ISE trust relationship is being maintained. This stage also includes the eighth stage of the RMF: monitor security controls (and the operational environment). The intent is to ensure up-to-date situational awareness of the security state of the ISE systems and the resulting risks to the organization, individuals, other organizations, and the Nation. It is essential for an effective sharing environment that trust, once established, be maintained over time, and the oversight and monitoring conducted as part of Stage Six of the ISE Architecture Implementation Life Cycle is where the actions necessary to achieve ongoing trust are executed.

3.7.2.2 Architecture

Operations and maintenance activities entail the day-to-day support activities that ensure data, service, and application assets are reliable and functional. During this activity, an operations and maintenance (O&M) guidebook should be created.

ISE participants should use the following high level procedures to complete O&M activity:

1. Develop an O&M guidebook.
2. Leverage administrative and managerial tools to monitor and maintain shared assets.
3. Provide alerts and postings regarding system outages or planned maintenance.
4. Develop feedback mechanisms to gather user feedback.

As the ISE is used by more participants, feedback on shared assets facilitates identification of new areas to address. This feedback eventually leads into subsequent iterations of the ISE Architecture Implementation Life Cycle. This stage allows the ISE to mature and evolve into a more robust, reliable system. The governing body of the ISE and each Core Service will be responsible for supporting the actual operations and maintenance of the ISE.

During Stage Six, data are collected regarding ISE participation performance. Ten ISE Baseline Measures are spread among five measurement categories. Once the measures are finalized and approved, they will be incorporated into both the ISE EAF v2.0 and the OMB FTF Catalog and should serve as a template for developing ISE performance metrics.

3.7.3 Implementation Agent Considerations

This is the stage (Stage Six) at which ISE Implementation Agents will enter the O&M phase of the service or core capabilities for which they are responsible. In many cases this responsibility requires that Implementation Agents will be primarily focused on maintaining their quality of service, extending their support to new ISE participants (individuals or organizations), evaluating their quality of service, and improving and extending their service as required.

Typically, the Implementation Agent will begin by preparing and executing a detailed performance evaluation plan and collecting and tracking performance metrics in parallel with the conduct of daily operations tasks such as maintenance of service, security monitoring, on-going privacy evaluation and protection, user/access management, etc. The performance evaluation plan will usually be coordinated with other ISE participants who are directly affected and will include opportunities for those participants to provide direct input.

It is critical, at this stage, that Implementation Agents be mindful of opportunities to add capabilities or features to their service or core capabilities that further the general goals of the ISE. Additions can include, for example, embracing new requirements that implement new and emerging collaborative technologies or opportunities to leverage emerging internal capabilities in a collaborative manner. Implementation Agents, at this stage, also need to consider participating in larger periodic ISE evaluations, assessments, and planning activities.

3.7.4 Outputs/Outcomes

Outputs: Stage Six yields documentation regarding O&M of the shareable assets. Primarily, it provides guidance on administrative and management functions and feedback mechanisms.

Outcomes: The desired outcomes for this stage are

- On-going, up-to-date situational awareness that accurately reflects the state of the ISE information system(s) and the ISE operational environment
- All affected authorizing officials have the information necessary for objective grounds for confidence that authorization decisions remain valid, or if not, that necessary corrective actions are being initiated

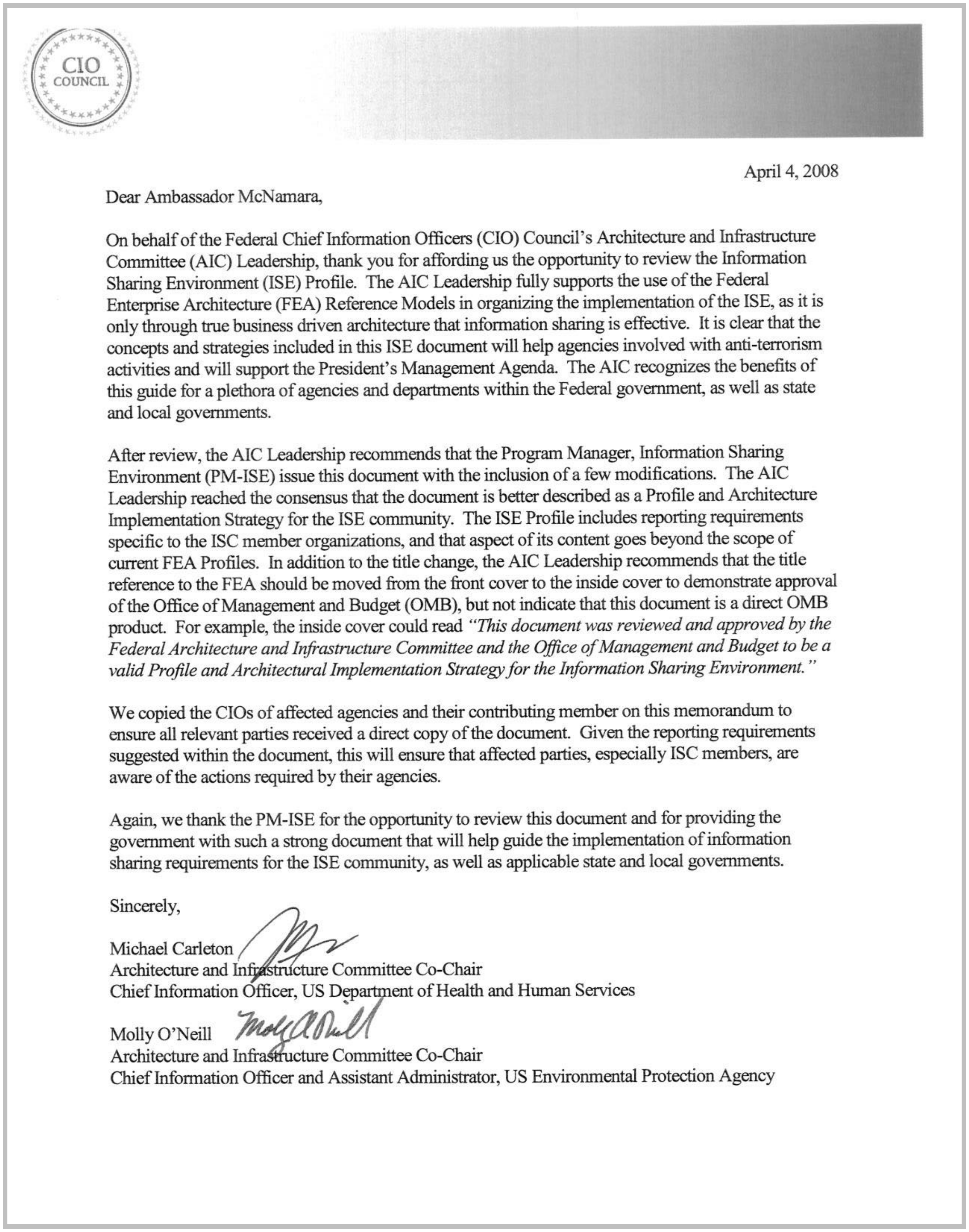
This page intentionally blank.

INFORMATION SHARING ENVIRONMENT PROFILE AND ARCHITECTURE IMPLEMENTATION STRATEGY

APPENDICES

This page intentionally blank.

Appendix A – Architecture and Infrastructure Committee Letter



CIO COUNCIL

April 4, 2008

Dear Ambassador McNamara,

On behalf of the Federal Chief Information Officers (CIO) Council's Architecture and Infrastructure Committee (AIC) Leadership, thank you for affording us the opportunity to review the Information Sharing Environment (ISE) Profile. The AIC Leadership fully supports the use of the Federal Enterprise Architecture (FEA) Reference Models in organizing the implementation of the ISE, as it is only through true business driven architecture that information sharing is effective. It is clear that the concepts and strategies included in this ISE document will help agencies involved with anti-terrorism activities and will support the President's Management Agenda. The AIC recognizes the benefits of this guide for a plethora of agencies and departments within the Federal government, as well as state and local governments.

After review, the AIC Leadership recommends that the Program Manager, Information Sharing Environment (PM-ISE) issue this document with the inclusion of a few modifications. The AIC Leadership reached the consensus that the document is better described as a Profile and Architecture Implementation Strategy for the ISE community. The ISE Profile includes reporting requirements specific to the ISC member organizations, and that aspect of its content goes beyond the scope of current FEA Profiles. In addition to the title change, the AIC Leadership recommends that the title reference to the FEA should be moved from the front cover to the inside cover to demonstrate approval of the Office of Management and Budget (OMB), but not indicate that this document is a direct OMB product. For example, the inside cover could read *"This document was reviewed and approved by the Federal Architecture and Infrastructure Committee and the Office of Management and Budget to be a valid Profile and Architectural Implementation Strategy for the Information Sharing Environment."*

We copied the CIOs of affected agencies and their contributing member on this memorandum to ensure all relevant parties received a direct copy of the document. Given the reporting requirements suggested within the document, this will ensure that affected parties, especially ISC members, are aware of the actions required by their agencies.

Again, we thank the PM-ISE for the opportunity to review this document and for providing the government with such a strong document that will help guide the implementation of information sharing requirements for the ISE community, as well as applicable state and local governments.

Sincerely,

Michael Carleton
Architecture and Infrastructure Committee Co-Chair
Chief Information Officer, US Department of Health and Human Services

Molly O'Neill Molly O'Neill
Architecture and Infrastructure Committee Co-Chair
Chief Information Officer and Assistant Administrator, US Environmental Protection Agency

This page intentionally blank.

Appendix B – Acronyms

AIC	Architecture and Infrastructure Committee
AJAX	Asynchronous JavaScript and Extensible Markup Language
APHS-CT	Assistant to the President for Homeland Security and Counterterrorism
APNSA	Assistant to the President for National Security Affairs
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ASP	Application and Service Partition
AWG	Architecture Working Group
BATS	Bomb Arson Tracking System
BGP	Border Gateway Protocol
BP	Business Process
BPEL4WS	Business Process Execution Language for Web Services
BPM	Business Process Model
BPMN	Business Process Modeling Notation
BRM	Business Reference Model
BPR	Business Process Reengineering
C&A	Certification and Accreditation
CCEA	Continuity Communications Enterprise Architecture
CDMO	Cross-Domain Management Office
CDS	Cross-Domain Solution
CEA	Chief Enterprise Architect
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
COI	Community of Interest
CONOPS	Concept of Operations
COOP	Continuity of Operations Planning
COP	Committee of Principals
COTS	Commercial Off-the-Shelf
CPIC	Capital Planning and Investment Control
CRM	Consolidated Reference Model
CT	Counterterrorism
CTISS	Common Terrorism Information Sharing Standards
CTISSWG	CTISS Working Group

CVS	Certificate Validation Service
CY	Calendar Year
DDMS	DoD Discovery Metadata Specification
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DNI	Director of National Intelligence
DoD	Department of Defense
DOI	Department of the Interior
DOJ	Department of Justice
DOS	Department of State
DRM	Data Reference Model
EA	Enterprise Architecture
EAF	Enterprise Architecture Framework
EDS	Electronic Directory Services
EO	Executive Order
ESM	Enterprise Services Management
ETL	Extract, Translate, and Locate
FAQ	Frequently Asked Questions
FBI	Federal Bureau of Investigation
FEA	Federal Enterprise Architecture
FEAF	Federal Enterprise Architecture Framework
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FSI	Foreign Service Institute
FTF	Federal Transition Framework
FY	Fiscal Year
GIG	Global Information Grid
GJXDM	Global Justice Extensible Markup Language Data Model
GOTS	Government-Off-the-Shelf
HAIPE	High Assurance Internet Protocol Encryptor
HazMat	Hazardous Material

HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Over Secure Socket Layer
IA	Information Assurance
IA	Implementation Agent
IC	Intelligence Community
IDS	Intrusion Detection System
IEP	Information Exchange Package
IEPD	Information Exchange Package Documentation
ILC	Implementation Life Cycle
IMP	Information Sharing Environment Management Portal
IP	Implementation Plan
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Security Protocol
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISC	Information Sharing Council
ISE	Information Sharing Environment
ISEEA	Information Sharing Environment Enterprise Architecture
ISM	Information Security Markings
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
IT	Information Technology
ITACG	Interagency Threat Assessment and Coordination Group
ITIA	Information Technology Implementation Agent
JTF	Joint Task Force
JWICS	Joint Worldwide Intelligence Communications System
LoB	Line of Business
NCES	Net-Centric Enterprise Services
NCS	National Communications System
NCTC	National Counterterrorism Center
NIEM	National Information Exchange Model
NIPRNet	Non-classified Internet Protocol Router Network

NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
O&M	Operations and Maintenance
OMB	Office of Management and Budget
PAIS	Profile and Architecture Implementation Strategy
PDS	Policy Decision Service
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
PM	Program Manager
PM-ISE	Program Manager, Information Sharing Environment
PMO	Program Management Office
PRM	Performance Reference Model
PRS	Policy Retrieval Service
QoS	Quality of Service
RM	Reference Model
RMF	Risk Management Framework
S	Secret (Security Classification)
SAR	Suspicious Activity Report
SBU	Sensitive But Unclassified (Security Classification)
SCI	Special Compartmented Information (Security Classification)
SDLC	Systems Development Life Cycle
SGML	Standard Generalized Markup Language
SIPRNet	Secret Internet Protocol Router Network
SIR	Suspicious Incident Report
SLA	Service Level Agreement
SLT	State, Local, and Tribal
SOAP	Simple Object Access Protocol
SP	Special Publication
SRM	Service Component Reference Model

SSP	System Security Plan
T&E	Test and Evaluation
TRM	Technical Reference Model
TTL	Time-to-Live
TWPDES	Terrorist Watchlist Person Data Exchange Standard
UDDI	Universal Description, Discovery, and Integration
UI	User Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VOIP	Voice Over Internet Protocol
W3C	World Wide Web Consortium
WAN	Wide Area Network
WG	Working Group
WMD	Weapons of Mass Destruction
WSDL	Web Services Description Language
XACML	Extensible Access Control Markup Language
XML	Extensible Markup Language

This page intentionally blank.

Appendix C – Bibliography

1. Executive Office of the President, Office of Management and Budget, *Federal Transition Framework*. See http://www.whitehouse.gov/omb/egov/a-2-EAFTF.html for latest version.

2. *Federal Enterprise Architecture Consolidated Reference Model*, Version 2.0, June 2006. http://www.whitehouse.gov/omb/egov/a-2-EAModelsNEW2.html

3. *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law No. 108-458, 118 Stat. 3638 (December 17, 2004). http://www.nctc.gov/docs/pl108_458.pdf

4. *National Security Act of 1947*, as amended (50 U.S.C. 402 et seq.). http://www.intelligence.gov/0-natsecact_1947.shtml

5. Executive Office of the President, *Office of Management and Budget (OMB), Preparation, Submission, and Execution of the Budget*, Circular No. A-11, June 2006. http://www.whitehouse.gov/omb/circulars/a11/current_year/a11_toc.html

6. Office of Management and Budget (OMB), *Memorandum for Heads of Executive Departments and Agencies, Subject: Management of Federal Information Resources*, Circular No. A-130, Revised, (Transmittal Memorandum No. 4). http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf

7. The President, *Further Amendment to Executive Order 12958, as Amended, Classified National Security Information*, Executive Order 13292, March 25, 2003. http://www.whitehouse.gov/news/releases/2003/03/20030325-11.html

8. Program Manager, *Information Sharing Environment, Information Sharing Environment Enterprise Architecture Framework*, August 2007. http://www.ise.gov/docs/eaf/ISE-EAF_v1.0_20070830.pdf

9. Program Manager, *Information Sharing Environment, Information Sharing Environment Implementation Plan*, November 2006. http://www.ise.gov/docs/reports/ise-impplan-200611.pdf

10. Program Manager, *Information Sharing Environment, The Information Sharing Environment Interim Implementation Plan*, January 2006. http://www.ise.gov/docs/reports/ise_interim_implementation_plan-20060109.pdf

11. Executive Office of the President, Office of Management and Budget, *Federal Enterprise Architecture Program EA Assessment Framework 2.2*, October 2007, available at http://www.whitehouse.gov/omb/egov/a-2-EAAssessment.html.

12. Office of the DNI/CIO, *Common Information Sharing Standard for Tearline Applications: XML Implementation*, Release 1.0, November 2004.

13. Office of the DNI/CIO, Common Information Sharing Standard for Tearline Applications: Messaging Implementation, Release 1.1, November 2004.

14. Hohpe Gregor and Bobby Woolf (2003). *Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions*. ISBN 0-321-20068-3.

Appendix D – Glossary

Access Control—Limiting access to information system resources only to authorized users, programs, processes, or other systems. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Agency Transport—That infrastructure (including cabling, network components, and protocols) that enables the movement of data between agencies participating in the ISE.

Agency—Has the meaning set forth for the term “executive agency” in section 105 of title 5, United States Code (i.e., an Executive department, a Government corporation, and an independent establishment), together with the Department of Homeland Security, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government Accountability Office. [EO 13388 Section (6)(a) and 5 U.S.C. 105]

Application Architecture—The high-level design that defines the major components of a software application, the information that flows between those components, and the transformations that those components apply to that information.

Audit—Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures and to recommend necessary changes in controls, policies, or procedures.

Audit Trail Capture and Analysis—Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Authentication—Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual’s authorization to receive specific categories of information. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Authorization—Access privileges granted to a user, program, or process. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Availability—Timely, reliable access to data and information services for authorized users. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Business Analytical Services—Supports “the extraction, aggregation, and presentation of information to facilitate decision analysis.” [http://www.whitehouse.gov/omb/egov/documents/FEA_CRM_v23_Final_Oct_2007.pdf]

Business Architecture—An inventory of agency business processes, aligned to the FEA Business Reference Model (BRM), linked to layers of the agency EA, and used to inform investment decision making. [http://www.whitehouse.gov/omb/egov/documents/OMB_EA_Assessment_Framework_v22_Final.pdf]

Business Reference Model—A framework facilitating a functional (not organizational) "view of the Federal Government's lines of business (LoBs), including its internal operations and its services for citizens, independent of the agencies, bureaus, and offices that perform them." [http://www.whitehouse.gov/omb/egov/documents/FEA_CRM_v23_Final_Oct_2007.pdf]

Common Services—In a service-oriented architecture, Web services are divided into two broad categories: Line of Business Services and Common Services. Common Services are those services employed by a large subset of users. These services are provided centrally by an enterprise authority to assure interoperability and maximize reuse.

Community of Interest (COI)—COI is defined in the National Information Exchange Model (NIEM) Concept of Operations (CONOPS), October 2004, as a collaborative group of users who require a shared vocabulary to exchange information in pursuit of common goals, interests, and business objectives.

Confidentiality—Assurance that information is not disclosed to unauthorized individuals, processes, or devices. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Continuity of Operations Planning (COOP)—Plan for continuing an organization's (usually a headquarters element) essential functions at an alternate site and performing those functions for the duration of an event with little or no loss of continuity before returning to normal operations. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Controlled Unclassified Information (CUI)—Categories of unclassified information that require controls that protect the information from public release, both to safeguard the civil liberties and legal rights of U.S. citizens and to deny information advantage to those who threaten the security of the Nation.

Core Enterprise Services (CES)—Services that enable both service and data providers on the "net," by providing and managing the underlying capabilities to deliver content and value to end-users.

Cross-Agency Initiative—An effort supported with resources (including staff, products, information, and/or funding) from multiple Federal agencies for the mutual benefit of all.

Cross-Domain Security—An integrated, comprehensive, and consistent approach to addressing the shared risk associated with the connection of networks of different classification levels.

Data Accessibility—Those functional capabilities of the ISE that allow a user of the ISE to obtain data when needed. In particular, data accessibility depends on the principles that all data shall be posted to ISE Shared Spaces and tagged with metadata to enable access to all users except when limited by security, policy, or regulations.

Data Context—Any information that provides additional meaning to data. Data Context typically specifies a designation or description of the application environment or discipline in which data is applied or from which it originates. It provides perspective, significance, and connotation to data and is vital to the discovery, use, and comprehension of data. [http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf]

Data Description—A rich description of data, thereby supporting its discovery and sharing. [http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf]

Data Interoperability—The capability of different programs to exchange data via a common set of business procedures and to read and write the same file formats and use the same protocols.

Data-in-Transit—Data is typically referred to as being in one of three states at any time: (1) at rest, (2) processing, or (3) in transit. Data-in-Transit refers to the state in which data is being passed from one physical location to another via the ISE Transport. Data is in transit when it is passing over physical cables, being transmitted over wireless networks and satellite links, and passing through routers and other network components.

Data Reference Model (DRM)—One of the five reference models of the Federal Enterprise Architecture (FEA). The DRM is a framework whose primary purpose is to enable information sharing and reuse across the Federal Government via the standard description and discovery of common data and the promotion of uniform data management practices. [http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf]

Data Sharing—Describes the sharing and exchange of data, where sharing may consist of ad-hoc requests (such as a one-time query of a particular data asset), scheduled queries, and/or exchanges characterized by fixed, re-occurring transactions between parties. It involves exchanges within and between agencies and COIs to support mission-critical capabilities. Finally, it eliminates duplication and/or replication of data, thereby increasing data quality and integrity. [http://www.whitehouse.gov/omb/egov/documents/DRM_2_0_Final.pdf]

Data Trustability—Those functional capabilities of the ISE that enable a user to place a value on specific data provided in the ISE. In particular, Data Trustability depends on the principle that data shall be tagged with metadata describing its pedigree, source, timeliness, confidence, or other attributes associated with trust.

Data Understandability—The functional capabilities of the ISE that enable a user to properly interpret specific data and use that data in an appropriate manner. In particular Data Understandability depends on the principle that data shall be tagged with metadata describing its pedigree, source, timeliness, and perhaps description. Even more important, however, is that data be described in standard ways using common terminology as established by negotiated and accepted taxonomies.

Data Visibility—The functional capabilities of the ISE that reveal the existence of specific data to a user of the ISE. In particular, data visibility depends on the principles that all data shall be posted to ISE Shared Spaces and tagged with metadata to enable discovery of data by users.

Digital Signature—Cryptographic process used to assure message originator authenticity, integrity, and non-repudiation. Synonymous with electronic signature. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Domain—A virtual environment governed by a single set of consistent policies. These policies include, but need not be limited to, security policies that govern authentication, authorization, availability, confidentiality, and integrity. Typically a domain is managed by a single organizational entity, such as a single agency, that enforces the applicable policies, e.g., the CIA domain. A group of agencies may also establish a new domain for sharing information by agreeing on a consistent set of policies for the data stored in that domain and designating a proxy to manage that domain, e.g., the Intelligence Domain.

Domain Routing—The functionality that allows data to cross domain borders. For example, data may be routed from a Secret domain to a Sensitive But Unclassified domain through a trusted guard that enables specified policies for the declassification of information. In the near term, a routing protocol domain boundary will be established at these administrative domain boundaries.

Enabling Technology—Any technological capability used to support ISE policies or business processes.

Encryption—The process of obscuring information to make it unreadable without special knowledge.

Enterprise Architecture—A strategic information asset base that defines the mission, the information necessary to perform the mission and the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs.

Enterprise Search—The act of searching content to discover data, information, and knowledge wherever it exists.

Extensible Markup Language (XML)—XML is a simple, flexible text format derived from Standard Generalized Markup Language (SGML). Originally designed to meet the challenges of large-scale electronic publishing, XML also plays an increasingly important role in the exchange of a wide variety of data on the Web and elsewhere. [http://www.w3.org/XML/]

Federal Enterprise Architecture—A business-driven framework that defines and aligns Federal business functions and supporting technology and includes a set of five common models (performance, business, service component, data, and technical).

Foreign Partners—Refers to non-U.S. government organizations that participate in the ISE. The term "foreign governments" is a general term that includes foreign governments and their sub-components, such as individual ministries or foreign provincial or local authorities. Such foreign partners include, for example, regional inter-governmental organizations such as the European Union (EU); international organizations composed of governments such as the United Nations (UN) and the International Criminal Police Organization (INTERPOL); certain other entities with recognized comparable international status and certain foreign private entities such as port operators, foreign airlines, and other logistics providers. [Foreign Government Information Sharing Working Group Report]

Fusion Center—A center established by State and major urban area governments designed to coordinate the gathering, analysis, and dissemination of terrorist-related, law enforcement, and public-safety information.

Global Information Grid (GIG)—Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

Homeland Security Information—Any information possessed by a Federal, State, or local agency that (A) relates to the threat of terrorist activity; (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (D) would improve the response to a terrorist act. [Section 892(f)(1) of the Homeland Security Act (6 U.S.C. 482(f)(1))]

Information Assurance—Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Information Sharing Council (ISC)—The Information Sharing Council was established by Executive Order 13356, or any successor body designated by the President, and referred to under subsection 1016(g) of the IRTPA. [Extracted from IRTPA 1016(a)(1)] EO 13388, which superseded EO 13356, established the Information Sharing Council.

Information Sharing Environment (ISE)—An approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section [1016]. [IRTPA 1016(a)(2)]

Integrity—Quality of an information system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.
[http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Intelligence Community Enterprise Architecture (ICEA)—Establishes the interoperability framework between the organizational/mission enterprise architecture necessary to support the business of intelligence.

Interoperability—The capability of different programs to exchange data via a common set of business procedures and to read and write the same file formats and use the same protocols.

Intrusion Detection—The act of detecting actions that attempt to compromise the confidentiality, integrity, or availability of a resource. It does not necessarily prevent intrusion from occurring.

ISE Participant—Any Federal, State, local, or tribal government organization; private sector entity; or foreign government organization that participates in the ISE.

ISE Transport—That infrastructure (including cabling, network components, and protocols) that enables the movement of data between agencies participating in the ISE (synonymous with Agency Transport).

Law Enforcement Information—For the purposes of the ISE only, any information obtained by or of interest to a law enforcement agency or official that is both (A) related to terrorism or the security of our homeland and (B) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Line of Business—Internal operations of the Federal Government and its services, independent of the agencies that perform them. [http://www.whitehouse.gov/OMB/egov/documents/DRM_2_0_Final.pdf]

Local Government—Refers to (A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under state law), regional or interstate government entity, or agency or instrumentality of a local government; (B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and (C) a rural community, unincorporated town or village, or other public entity. [Homeland Security Act of 2002, 6 U.S.C. 101]

National Information Exchange Model (NIEM)—An interagency initiative to provide the foundation and building blocks for national-level interoperable information sharing and data exchange.

Net-centricity—Robust networks without central weakness versus centralized chains that can be cut or broken. Interoperable communications versus "stove-piped" communications infrastructure. Dynamic-situational security versus fixed-domain specific-security. Pull assured information versus push information out. Handle information only once versus multiple times, creating duplicate entries.

Non-repudiation—Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. [http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf]

Outcome Measures—Outcomes describe the intended result of carrying out a program or activity. They define an event or condition that is external to the program or activity and that is of direct importance to the intended beneficiaries and/or the public. [OMB A-11]

Person of Interest (POI)—A person or entity about which users of the ISE wish to obtain or share information (this term is used interchangeably with Target of Interest in this context).

Private Sector Partners—Includes vendors, owners, and operators of products and infrastructures participating in the ISE.

Program Manager—The program manager designated under subsection 1016(f) of the IRTPA, who is responsible for information sharing across the Federal Government and shall, in consultation with the Information Sharing Council, plan for and oversee the implementation of, and manage, the ISE. [Extracted from IRTPA 1016(a)(3) and 1016(f)]

Quality of Service—The probability of the telecommunication network meeting a given traffic contract, or in many cases a term used informally to refer to the probability of a packet succeeding in passing between two points in the network within its desired latency period.

Role/Privilege Management—Set of functions that protects networks and systems from unauthorized access by persons, acts, or influences and includes many sub-functions, such as creating, deleting, and controlling security services and mechanisms; distributing security-relevant information; reporting security-relevant events; controlling the distribution of cryptographic keying material; and authorizing subscriber access, rights, and privileges.

Security Domain—The term “Security Domain” refers to three security levels—Special Compartmented Information (SCI), Secret, and Sensitive but Unclassified (SBU)—across which the ISE must operate.

Segment—Segments are individual elements of the enterprise describing core mission areas and common or shared business services and enterprise services. Segments are defined by the enterprise architecture.

Service—Services provide a standard means of interoperating between different software applications that run on a variety of platforms and/or frameworks. Services are characterized by their interoperability and extensibility. They can be combined in a loosely coupled way in order to achieve complex operations. Programs providing simple services can interact with each other in order to deliver sophisticated added-value services. [http://www.w3.org/2002/ws/Activity]

Service Adaptation—Solves the problem of converting between the rules used by one service into those required by another while maintaining the integrity of the message being sent through the service-based architecture. [http://www.nces.dod.mil/coreServices/mediation_content.aspx]

Service-based Architecture—A business-driven approach to software architecture that supports integrating the business as a set of linked, repeatable business tasks, or “services.” Services are self-contained, reusable software modules with well-defined interfaces and are independent of applications and the computing platforms on which they run. Service-based architecture helps users build composite applications, which are applications that draw upon functionality from multiple sources within and beyond the enterprise to support horizontal business processes.

Service Level Agreement (SLA)—SLA defines mutual understandings and expectations between a service consumer and a service provider. The service-level objectives that both the service consumer and the service provider agree upon usually include a set of indicators such as availability and average response time.

Shared Data—The terrorism data collected and maintained by agencies in the course of executing their mission.

Simple Object Access Protocol (SOAP)—SOAP Version 1.2 is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. The "Messaging Framework" component defines, using XML technologies, an extensible messaging framework containing a message construct that can be exchanged over a variety of underlying protocols. [http://www.w3.org/TR/soap12-part1/]

State—Any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States. [Homeland Security Act of 2002, 6 U.S.C. 101]

Suspicious Activities Report (SAR)—Official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention (ISE-FS-200: ISE-SAR Functional Standard found at www.ise.gov).

Target of Interest (TOI)—A person or entity of significance, under watch or investigation, who could pose a threat to the United States or U.S. interests.

Technical Architecture—This component characterizes hardware, operating systems, programming, and network solutions used across the ISE.

Technical Reference Model (TRM)—A component-driven, technical framework used to categorize the standards, specifications, and technologies that support and enable the delivery of service components and capabilities. The TRM provides a foundation to categorize the standards, specifications, and technologies to support the construction, delivery, and exchange of business and application components that may be used and leveraged in a Component-Based or Service-Oriented Architecture. It also unifies existing agency TRMs and Electronic Government (EGOV) guidance by providing a foundation to advance the re-use of technology and component services from a Government-wide perspective. [http://www.whitehouse.gov/omb/egov/documents/FEA_CRM_v23_Final_Oct_2007.pdf]

Terrorism Information—All information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (B) threats posed by such groups or individuals to the United States, United States persons, United States interests, or to those of other nations; (C) communications of or by such groups or individuals; or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals. [IRTPA 1016(a)(4)]

User Applications—Software applications used by one or more ISE user communities wishing to leverage the capabilities of the ISE. User Applications is in contrast to

Enterprise Applications, which are used by a large subset of ISE users and provided centrally, or Management Applications, which are used by a small set of administrators to maintain and operate the ISE.

Virtual Private Network (VPN)—A private communications network usually used within a company, or by several different companies or organizations, to communicate from remote locations over an insecure public network.

Web Service Description Language (WSDL)—WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate. [http://www.w3.org/TR/wsdl]

XML Schemas/XML Schema Definitions (XSD)—Express shared vocabularies and allow machines to carry out rules made by people. They provide a means for defining the structure, content, and semantics of XML documents.
[http://www.w3.org/XML/Schema]

Appendix E – ISE Business Processes

Mission Business Processes	
Information Requirements and Roles	Supports handling of terrorism information requirements from ISE participants and prioritization of needs and allocation of resources. Provides status of actions against requirements. Feeds program and budget-planning processes for long term investments.
Alerts and Notifications	Supports the preparation of and ensures timely dissemination and handling of terrorism alerts and warnings among ISE participants, at appropriate security levels.
Suspicious Activity Reporting	Reports observed behavior that maybe indicative of intelligence gathering or pre-operational planning related to terrorism, criminal espionage, and other illicit information.
Identification and Screening	Supports the counterterrorism (CT) community efforts to identify and screen personnel and material. This includes updates of terrorist watch-lists and making them availability to ISE participants when needed. Ensures watch-list entries are consistent and current. It also encompasses effort to identify and screen shipments for entry control into the U.S. or U.S. controlled areas; for verifying eligibility to selected public and private sector services; and for LE actions.
Analysis	Provides support as needed to analytic processes employed by ISE participants.
Operations	Provides ISE support to a variety of ISE operational activities, including collection, investigations, and inspections.
Policy and Decision Making	Supports policy maker information needs and other counterterrorism decision processes. Contributes fusion of disparate data into a strategic picture that allows decision makers to collaborate on possible courses of action and to preempt or to respond to events as necessary.
Response	Supports the counterterrorism community effort to respond (act) on a terrorism-related threat.
Protection	Supports the counterterrorism community effort to protect the territory people, and interests of the United States.
Service Business Processes	
Access	A process used to grant an individual access to information and associated resources of ISE member Communities based on verification of the individual's identity and associated attributes (Identity Management). The Access Process must ensure security and currency of credentialing and mission role information. It also protects personal identity information where applicable.
Discovery and Search	Allow ISE participants to conduct queries of disparate terrorism-related information; support ISE participants' ability to discover data from sources a participant may otherwise not know exists.

Service Business Processes (Continued)	
Dissemination	The process supports timely dissemination of terrorism information at the appropriate level of classification to ISE participants. The process supports data push, data pull and web-type posting of terrorism information. The Dissemination Process supports many ISE missions. In particular, it supports the Alert and Warnings Process by delivering information to various communication outlets – both governmental and public/private sector.
Collaboration	The business processes and supporting applications that enable people to interactively work together analyzing and acting upon terrorism-related information.
Manipulation and Storage	Provide tools and techniques to organize or catalog information in a structured format that is searchable by other ISE participants. Satisfy mission needs for user response times with some combination of fast (on-line) and archival-type storage. Accommodate differences in Agency taxonomies with some combination of standards, limited common shareable data and/or mediation services to translate data between supplier and requestor ontologies. Establish link-ability between searchable data structure and actual data repositories.
Electronic Directory Services	A product that assists in locating people and organizations related to or supporting the counterterrorism mission.
Information Protection/Assurance	Ensure that the sharing environment accords at least the same level of system protection to terrorism-related information as is provided today to protect privacy and Civil Liberties.
Enabling Business Processes	
Issuances	Identify need for issuance; develop drafts; review and resolve; issue publication; monitor compliance.
Information Sharing Agreements	Provide common approaches for managing information sharing agreements between ISE participants.
Business Process and Performance Management	Identify problems in existing processes or need, assess impact, analyze and develop options for action, implement selected course of action, and monitor performance. Develop ISE-wide performance measures, monitor progress, ensure that department and agency goals and measures support ISE goals, prepare and publish annual ISE performance report.
Training/Cultural Change	Develops and executes ISE-wide training; provides guidance on, develops, implements, and monitors information sharing incentives.
Security Framework	Develops and implements a framework to ensure that terrorism information is handled securely and efficiently. (Specifically includes appropriate mechanisms to handle SBU and classified terrorism information.) Removes impediments to ISE clearances and visit handling, leverages C&A improvement, adopts and implements cross-domain solutions.
Standards and Architecture	Develop and maintain the ISE Enterprise Architecture Framework, the ISE Profile and Architecture Implementation Strategy (PAIS), and common standards.

Enabling Business Processes (Continued)	
Privacy and Civil Liberties Protection	Provides procedures and capabilities to ensure that privacy and civil liberties requirements are addressed in ISE.
ISE Governance and Management	Ensure that ISE governance process functions effectively and efficiently. This category includes processes that support ISE budgeting, auditing, and quality assurance.

This page intentionally blank.

Appendix F – Summary of Recommended Actions

[For ISE participants and Implementation Agents, the following actions are recommended.]

Recommended Action	Summary Description	ISE PAIS Reference
Identify goals and objectives for information sharing	A foundation of trust	2.1.5 3.2.2
Develop use cases for each shareable asset	Use cases bridge requirements to business processes.	3.2.2
Define the mission needs for information sharing	Identification of the mission needs for each ISE Implementation Agent and participant is the essential step to identifying the cross-agency "To-Be" business processes.	3.2.2
Identify and analyze "As-Is" information sharing business processes	Identify the current methods employed to carry out information sharing information. Further, identify areas to improve based on ineffective, unused, or rigid processes.	3.2.2
Develop "To-Be" information sharing business processes	Using "As-Is" business processes, address known gaps by re-engineering business processes to align with those of the ISE.	3.2.2
Identify and agree upon the risk associated with information sharing activities	A foundation of trust	2.1.5 3.2.2
Categorize data, application and service, and technical assets	Categorize assets in accordance with ISE policy and guidance as to potential impacts upon organization, individuals, other organizations, and the Nation. Use FIPS 199 and SP 800-60 guidance.	2.1.1 3.3.2
Create inventory of shareable assets	Identify and document current information sharing assets within the organization that can be leveraged for the ISE. Additionally, accompanying asset description documents, service-level agreements, and information exchange package descriptions must be leveraged or developed.	3.3.2
Identify required assets to support "To-Be" information sharing business process	Identify required assets not in current inventory required to fill gaps in support of the "To-Be" information sharing business processes.	3.3.2
Develop segment architecture	Using asset inventory and business process analysis, develop a segment architecture to describe a business driven approach to information sharing in alignment with enterprise architecture.	3.3.3
Agree upon scope of trustworthiness required to mitigate risk	A foundation of trust	2.1.5 3.4.2

Recommended Action	Summary Description	ISE PAIS Reference
Apply NIST SP 800-53 process using ISE-specific control baselines	Determine information security requirements and level of trustworthiness and begin to implement the Risk Management Framework.	2.1.1 3.4.2
Prepare shareable asset summary information	Prepare information in regard to each shareable asset. Additionally provide an analysis that illustrates how investment in these assets closes identified performance gaps.	3.4.2
Identify whether assets exist in target EA, EA transition strategy, and segment architecture.	Identify whether each asset proposed for investment exists in current or targeted architecture. If it does not, prepare justification as to why it has been excluded.	3.4.2
Demonstrate alignment with ISE-EAF and FEA CRM	Summarize the purpose and business processes of each shareable asset and illustrate its alignment to the partitions and reference models of the ISE EAF and the FEA CRM respectively.	3.4.2
Perform alternative analysis	Evaluate custom- developed and vendor solutions. Prepare documentation in support of each alternative.	3.4.2
Document risk management strategy	Prepare RMF documentation in accordance with the guidance provided in the PAIS.	2.1.1 3.4.2
Generate a roadmap for each investment	Create a work breakdown structure, level of effort assessment, and rough order of magnitude.	3.4.2
Prepare baseline performance measures	Prepare baseline performance measures in accordance with those issued by the PM-ISE.	3.4.2
Implement RMF	Implement the different RMF artifacts created in the previous steps.	2.1.1 3.5.2
Develop information sharing assets	Using internal system development processes, develop the shareable assets for use in the ISE in support of the “To-Be” business processes.	3.5.2.
Develop test scripts and scenarios	This action includes activities such as functional requirement verification and development of test and evaluation scripts and scenarios.	1.4 3.5.2
Develop assurance case	The assurance case combines information from previous steps with assessments performed to document the grounds for confidence that intended functionality is implemented with the required level of quality.	3.6.2
Complete asset deployment	Following internal procedures, organizations should prepare to deploy their assets into the ISE. This process includes finalizing any accompanying documentation and performing end-user testing within the ISE Test & Evaluation Environment.	3.6.2
Develop training documentation	Develop training documentation in addition to delivery and feedback mechanisms.	3.6.2

Recommended Action	Summary Description	ISE PAIS Reference
Develop operations and maintenance documentation	Develop procedures for monitoring trust relationships, security controls, and general health of shareable assets. Establish COOP procedures.	3.7.2
Prepare performance measures reports	Using performance metrics created during planning stage, develop detailed performance measure reports.	3.7.2

This page intentionally blank.

This page intentionally blank.

Office of the Director of National Intelligence
Attention: Program Manager, Information Sharing Environment
Washington, D.C. 20511

(202) 331-2490

Visit us on the web at http://www.ise.gov